

Sparse Difference Resultant*

Wei Li, Chun-Ming Yuan, Xiao-Shan Gao
 KLMM, Academy of Mathematics and Systems Science
 Chinese Academy of Sciences, Beijing 100190, China
 {liwei, cmyuan, xgao}@mmrc.iss.ac.cn

Abstract

In this paper, the concept of sparse difference resultant for a transformally essential system of difference polynomials is introduced and its properties are proved. In particular, order and degree bounds for sparse difference resultant are given. Based on these bounds, an algorithm to compute the sparse difference resultant is proposed, which is single exponential in terms of the number of variables, the Jacobi number, and the size of the transformally essential system. Also, the precise order, degree, a determinant representation, and a Poisson-type product formula for difference resultants are given.

Keywords. Sparse difference resultant, difference resultant, Laurent transformally essential system, Jacobi number, single exponential algorithm.

1 Introduction

The resultant, which gives conditions for an over-determined system of polynomial equations to have common solutions, is a basic concept in algebraic geometry and a powerful tool in elimination theory [3, 7, 9, 17, 18, 26]. The concept of sparse resultant is originated from the work of Gelfand, Kapranov, and Zelevinsky on generalized hypergeometric functions, where the central concept of \mathcal{A} -discriminant is studied [16]. Kapranov, Sturmfels, and Zelevinsky introduced the concept of \mathcal{A} -resultant [19]. Sturmfels further introduced the general mixed sparse resultant and gave a single exponential algorithm to compute the sparse resultant [26, 27]. Canny and Emiris showed that the sparse resultant is a factor of the determinant of a Macaulay style matrix and gave an efficient algorithm to compute the sparse resultant based on this matrix representation [11]. A determinant representation for the sparse resultant was given by D’Andrea [8]. Recently, in [14], a rigorous definition for the differential resultant of $n + 1$ generic differential polynomials in n variables was presented [14] and also the theory of sparse differential resultants for Laurent differentially essential systems was developed [22, 23]. It is meaningful to generalize the theory of sparse resultant to difference polynomial systems.

In this paper, the concept of sparse difference resultant for a Laurent transformally essential system consisting of $n + 1$ Laurent difference polynomials in n difference variables

* Partially supported by a National Key Basic Research Project of China (2011CB302400) and by a grant from NSFC (60821002).

is introduced and its basic properties are proved. In particular, we give order and degree bounds for the sparse difference resultant. Based on these bounds, we give an algorithm to compute the sparse difference resultant. The complexity of the algorithm in the worst case is single exponential of the form $O(m^{O(nlJ^2)}(nJ)^{O(lJ)})$, where n, m, J , and l are the number of variables, the degree, the Jacobi number, and the size of the Laurent transformally essential system respectively. Besides these, the difference resultant is introduced and its basic properties are given, such as its precise order, degree, determinant representation, and Poisson-type product formula.

Although most properties for sparse difference resultants and difference resultants are similar to its differential counterpart given in [22, 23, 14], some of them are quite different in terms of descriptions and proofs. Firstly, the definition for difference resultant is more subtle than the differential case as illustrated by Problem 3.15 in this paper. Secondly, the criterion for transformally essential systems given in Section 3.3 is quite different and much simpler than its differential counterpart given in [23]. Also, a determinant representation for the difference resultant is given in Section 6, but such a representation is still not known for differential resultants [30, 25]. Finally, some properties are more difficult in the difference case. For instance, we can only show that the vanishing of the difference resultant is a necessary condition for the corresponding difference polynomial system to have a common nonzero solution. While, the sufficient condition part is still open. Also, there does not exist a definition for homogeneous difference polynomials, and the definition we give in this paper is different from its differential counterpart.

The rest of the paper is organized as follows. In Section 2, we prove some preliminary results. In Section 3, we first introduce the concepts of Laurent difference polynomials and Laurent transformally essential systems, and then define the sparse difference resultant for Laurent transformally essential systems. Then basic properties of sparse difference resultant are proved in Section 4. And in Section 5, we present an algorithm to compute the sparse difference resultant. Then we introduce the notion of difference resultant and give its basic properties in section 6. In Section 7, we conclude the paper by proposing several problems for future research.

2 Preliminaries

In this section, some basic notations and preliminary results in difference algebra will be given. For more details about difference algebra, please refer to [5, 21].

2.1 Difference polynomial ring

An ordinary difference field \mathcal{F} is a field with a third unitary operation σ satisfying that for any $a, b \in \mathcal{F}$, $\sigma(a + b) = \sigma(a) + \sigma(b)$, $\sigma(ab) = \sigma(a)\sigma(b)$ and $\sigma(a) = 0$ if and only if $a = 0$. We call σ the transforming operator of \mathcal{F} . If $a \in \mathcal{F}$, $\sigma(a)$ is called the transform of a and is denoted by $a^{(1)}$. And for $n \in \mathbb{Z}^+$, $\sigma^n(a) = \sigma^{n-1}(\sigma(a))$ is called the n -th transform of a and denoted by $a^{(n)}$, with the usual assumption $a^{(0)} = a$. By $a^{[n]}$ we mean the set $\{a, a^{(1)}, \dots, a^{(n)}\}$. A typical example of difference field is $\mathbb{Q}(x)$ with $\sigma(f(x)) = f(x + 1)$.

Let S be a subset of a difference field \mathcal{G} which contains \mathcal{F} . We will denote respectively by $\mathcal{F}[S]$, $\mathcal{F}(S)$, $\mathcal{F}\{S\}$, and $\mathcal{F}\langle S \rangle$ the smallest subring, the smallest subfield, the smallest

difference subring, and the smallest difference subfield of \mathcal{G} containing \mathcal{F} and S . If we denote $\Theta(S) = \{\sigma^k a \mid k \geq 0, a \in S\}$, then we have $\mathcal{F}\{S\} = \mathcal{F}[\Theta(S)]$ and $\mathcal{F}\langle S \rangle = \mathcal{F}(\Theta(S))$.

A subset \mathcal{S} of a difference extension field \mathcal{G} of \mathcal{F} is said to be *transformally dependent* over \mathcal{F} if the set $\{\sigma^k a \mid a \in \mathcal{S}, k \geq 0\}$ is algebraically dependent over \mathcal{F} , and is said to be *transformally independent* over \mathcal{F} , or to be a family of *difference indeterminates* over \mathcal{F} in the contrary case. In the case \mathcal{S} consists of one element α , we say that α is *transformally algebraic* or *transformally transcendental* over \mathcal{F} respectively. The maximal subset Ω of \mathcal{G} which are transformally independent over \mathcal{F} is said to be a *transformational transcendence basis* of \mathcal{G} over \mathcal{F} . We use $\Delta \text{tr.deg } \mathcal{G}/\mathcal{F}$ to denote the *difference transcendence degree* of \mathcal{G} over \mathcal{F} , which is the cardinal number of Ω . Considering \mathcal{F} and \mathcal{G} as ordinary algebraic fields, we denote the algebraic transcendence degree of \mathcal{G} over \mathcal{F} by $\text{tr.deg } \mathcal{G}/\mathcal{F}$.

Now suppose $\mathbb{Y} = \{y_1, y_2, \dots, y_n\}$ is a set of difference indeterminates over \mathcal{F} . The elements of $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[y_j^{(k)} : j = 1, \dots, n; k \in \mathbb{N}_0]$ are called *difference polynomials* over \mathcal{F} in \mathbb{Y} , and $\mathcal{F}\{\mathbb{Y}\}$ itself is called the *difference polynomial ring* over \mathcal{F} in \mathbb{Y} . A difference polynomial ideal \mathcal{I} in $\mathcal{F}\{\mathbb{Y}\}$ is an ordinary algebraic ideal which is closed under transforming, i.e. $\sigma(\mathcal{I}) \subset \mathcal{I}$. If \mathcal{I} also has the property that $a^{(1)} \in \mathcal{I}$ implies that $a \in \mathcal{I}$, it is called a *reflexive difference ideal*. And a prime (resp. radical) difference ideal is a difference ideal which is prime (resp. radical) as an ordinary algebraic polynomial ideal. For convenience, a prime difference ideal is assumed not to be the unit ideal in this paper. If S is a finite set of difference polynomials, we use (S) and $[S]$ to denote the algebraic ideal and the difference ideal in $\mathcal{F}\{\mathbb{Y}\}$ generated by S .

An n -tuple over \mathcal{F} is an n -tuple of the form $\mathbf{a} = (a_1, \dots, a_n)$ where the a_i are selected from some difference overfield of \mathcal{F} . For a difference polynomial $f \in \mathcal{F}\{y_1, \dots, y_n\}$, \mathbf{a} is called a *difference zero* of f if when substituting $y_i^{(j)}$ by $a_i^{(j)}$ in f , the result is 0. An n -tuple η is called a *generic zero* of a difference ideal $\mathcal{I} \subset \mathcal{F}\{\mathbb{Y}\}$ if for any polynomial $P \in \mathcal{F}\{\mathbb{Y}\}$ we have $P(\eta) = 0 \Leftrightarrow P \in \mathcal{I}$. It is well known that

Lemma 2.1 [5, p.77] *A difference ideal possesses a generic zero if and only if it is a reflexive prime difference ideal other than the unit ideal.*

Let \mathcal{I} be a reflexive prime difference ideal and η a generic point of \mathcal{I} . The *dimension* of \mathcal{I} is defined to be $\Delta \text{tr.deg } \mathcal{F}\langle \eta \rangle / \mathcal{F}$.

Given two n -tuples $\mathbf{a} = (a_1, \dots, a_n)$ and $\bar{\mathbf{a}} = (\bar{a}_1, \dots, \bar{a}_n)$ over \mathcal{F} . $\bar{\mathbf{a}}$ is called a *specialization* of \mathbf{a} over \mathcal{F} , or \mathbf{a} *specializes* to $\bar{\mathbf{a}}$, if for any difference polynomial $P \in \mathcal{F}\{\mathbb{Y}\}$, $P(\mathbf{a}) = 0$ implies that $P(\bar{\mathbf{a}}) = 0$. The following property about difference specialization will be needed in this paper.

Lemma 2.2 *Let $P_i(\mathbb{U}, \mathbb{Y}) \in \mathcal{F}\langle \mathbb{Y} \rangle \{\mathbb{U}\}$ ($i = 1, \dots, m$) where $\mathbb{U} = (u_1, \dots, u_r)$ and $\mathbb{Y} = (y_1, \dots, y_n)$ are sets of difference indeterminates. If $P_i(\mathbb{U}, \mathbb{Y})$ ($i = 1, \dots, m$) are transformally dependent over $\mathcal{F}\langle \mathbb{U} \rangle$, then for any difference specialization \mathbb{U} to $\bar{\mathbb{U}}$ which are elements in \mathcal{F} , $P_i(\bar{\mathbb{U}}, \mathbb{Y})$ ($i = 1, \dots, m$) are transformally dependent over \mathcal{F} .*

Proof: It suffices to show the case $r = 1$. Denote $u = u_1$. Since $P_i(u, \mathbb{Y})$ ($i = 1, \dots, m$) are transformally dependent over $\mathcal{F}\langle u \rangle$, there exist natural numbers s and l such that $\mathbb{P}_i^{(k)}(u, \mathbb{Y})$ ($k \leq s$) are algebraically dependent over $\mathcal{F}(u^{(k)} \mid k \leq s + l)$. When u specializes to $\bar{u} \in \mathcal{F}$, $u^{(k)}$ ($k \geq 0$) are correspondingly algebraically specialized to $\bar{u}^{(k)} \in \mathcal{F}$. By [29,

p.161], $\mathbb{P}_i^{(k)}(\bar{u}, \mathbb{Y})$ ($k \leq s$) are algebraically dependent over \mathcal{F} . Thus, $P_i(\bar{u}, \mathbb{Y})$ ($i = 1, \dots, m$) are transformally dependent over \mathcal{F} . \square

2.2 Characteristic sets for a difference polynomial system

Let f be a difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$. The order of f w.r.t. y_i is defined to be the greatest number k such that $y_i^{(k)}$ appears effectively in f , denoted by $\text{ord}(f, y_i)$. And if y_i does not appear in f , then we set $\text{ord}(f, y_i) = -\infty$. The *order* of f is defined to be $\max_i \text{ord}(f, y_i)$, that is, $\text{ord}(f) = \max_i \text{ord}(f, y_i)$.

A *ranking* \mathcal{R} is a total order over $\Theta(\mathbb{Y}) = \{\sigma^k y_i | 1 \leq i \leq n, k \geq 0\}$, which satisfies the following properties:

- 1) $\sigma(\theta) > \theta$ for all derivatives $\theta \in \Theta(\mathbb{Y})$.
- 2) $\theta_1 > \theta_2 \implies \sigma(\theta_1) > \sigma(\theta_2)$ for $\theta_1, \theta_2 \in \Theta(\mathbb{Y})$.

Let f be a difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$ and \mathcal{R} a ranking endowed on it. The greatest $y_j^{(k)}$ w.r.t. \mathcal{R} which appears effectively in f is called the *leader* of p , denoted by $\text{ld}(f)$ and correspondingly y_j is called the *leading variable* of f , denoted by $\text{lvar}(f) = y_j$. Let the degree of f in $\text{ld}(f)$ be d . The leading coefficient of f as a univariate polynomial in $\text{ld}(f)$ is called the *initial* of f and is denoted by I_f .

Let p and q be two difference polynomials in $\mathcal{F}\{\mathbb{Y}\}$. q is said to be of higher rank than p if

- 1) $\text{ld}(q) > \text{ld}(p)$, or
- 2) $\text{ld}(q) = \text{ld}(p) = y_j^{(k)}$ and $\deg(q, y_j^{(k)}) > \deg(p, y_j^{(k)})$.

Suppose $\text{ld}(p) = y_j^{(k)}$. q is said to be *reduced* w.r.t. p if $\deg(q, y_j^{(k+l)}) < \deg(p, y_j^{(k)})$ for all $l \in \mathbb{N}_0$.

A finite chain of nonzero difference polynomials $\mathcal{A} = A_1, \dots, A_m$ is said to be an *ascending chain* if

- 1) $m = 1$ and $A_1 \neq 0$ or
- 2) $m > 1$, $A_j > A_i$ and A_j is reduced w.r.t. A_i for $1 \leq i < j \leq m$.

Let $\mathcal{A} = A_1, A_2, \dots, A_t$ be an ascending chain with I_i as the initial of A_i , and f any difference polynomial. Then there exists an algorithm, which reduces f w.r.t. \mathcal{A} to a polynomial r that is reduced w.r.t. \mathcal{A} , satisfying the relation

$$\prod_{i=1}^t \prod_{k=0}^{d_i} (\sigma^k \text{I}_i)^{e_{ik}} \cdot f \equiv r, \text{ mod } [\mathcal{A}],$$

where the e_{ik} are nonnegative integers. The difference polynomial r is called the *difference remainder* of f w.r.t. \mathcal{A} [15].

Let \mathcal{A} be an ascending chain. Denote $\mathbb{I}_{\mathcal{A}}$ to be the minimal multiplicative set containing the initials of elements of \mathcal{A} and their transforms. The *saturation ideal* of \mathcal{A} is defined to be

$$\text{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbb{I}_{\mathcal{A}} = \{p : \exists h \in \mathbb{I}_{\mathcal{A}}, \text{ s.t. } hp \in [\mathcal{A}]\}.$$

And the *algebraic saturation ideal* of \mathcal{A} is $\text{asat}(\mathcal{A}) = (\mathcal{A}) : \mathbb{I}_{\mathcal{A}}$, where $\mathbb{I}_{\mathcal{A}}$ is the minimal multiplicative set containing the initials of elements of \mathcal{A} .

An ascending chain \mathcal{C} contained in a difference polynomial set \mathcal{S} is said to be a *characteristic set* of \mathcal{S} , if \mathcal{S} does not contain any nonzero element reduced w.r.t. \mathcal{C} . A characteristic set \mathcal{C} of a difference ideal \mathcal{J} reduces to zero all elements of \mathcal{J} .

Let \mathcal{A} be a characteristic set of a reflexive prime difference ideal \mathcal{I} . We rewrite \mathcal{A} as the following form

$$\mathcal{A} = \begin{cases} A_{11}, \dots, A_{1k_1} \\ \dots \\ A_{p1}, \dots, A_{pk_p} \end{cases}$$

where $\text{lvar}(A_{ij}) = y_{c_i}$ for $j = 1, \dots, k_i$ and $\text{ord}(A_{ij}, y_{c_i}) < \text{ord}(A_{il}, y_{c_i})$ for $j < l$. In terms of the characteristic set of the above form, p is equal to the *codimension* of \mathcal{I} , that is $n - \dim(\mathcal{I})$. Unlike the differential case, here even though \mathcal{I} is of codimension one, there may be more than one difference polynomials in a characteristic set of \mathcal{I} as shown by the following example.

Example 2.3 Let $A_{11} = (y_1^{(1)})^2 + y_1^2 + 1$, $A_{12} = y_1^{(2)} - y_1$. Then $\mathcal{I} = [A_{11}, A_{12}]$ is a reflexive prime difference ideal whose characteristic set is $\mathcal{A} = A_{11}, A_{12}$ and $\mathcal{I} = \text{sat}(\mathcal{A})$ [15]. Note that $[A_{11}]$ is not a prime difference ideal, because $\sigma(A_{11}) - A_{11} = (y_1^{(2)} - y_1)(y_1^{(2)} + y_1) \in [A_{11}]$ and both $y_1^{(2)} - y_1$ and $y_1^{(2)} + y_1$ are not in $[A_{11}]$.

Now we proceed to show that a property of uniqueness still exists in characteristic sets of a reflexive prime difference ideal in some sense. Firstly, we need several algebraic results.

Let $\mathcal{B} = B_1, \dots, B_m$ be an algebraic triangular set in $\mathcal{F}[x_1, \dots, x_n]$ with $\text{lvar}(B_i) = y_i$ and $U = \{x_1, \dots, x_n\} \setminus \{y_1, \dots, y_m\}$. A polynomial f is said to be invertible w.r.t. \mathcal{A} if $(f, A_1, \dots, A_s) \cap K[U] \neq \{0\}$ where $\text{lvar}(f) = \text{lvar}(A_s)$. We call \mathcal{B} a *regular chain* if for each $i > 1$, the initial of B_i is invertible w.r.t. B_1, \dots, B_{i-1} . For a regular chain \mathcal{B} , we say that f is invertible w.r.t. $\text{sat}(\mathcal{B})$ if $(f, \text{sat}(\mathcal{B})) \cap \mathcal{F}[U] \neq \{0\}$.

Lemma 2.4 Let \mathcal{B} be a regular chain in $\mathcal{F}[x_1, \dots, x_n]$. If $\sqrt{\text{sat}(\mathcal{B})} = \bigcap_{i=1}^m \mathcal{P}_i$ is an irredundant prime decomposition of $\sqrt{\text{sat}(\mathcal{B})}$, then a polynomial f is invertible w.r.t. $\text{sat}(\mathcal{B})$ if and only if $f \notin \mathcal{P}_i$ for all $i = 1, \dots, m$.

Proof: Since $\sqrt{\text{sat}(\mathcal{B})} = \bigcap_{i=1}^m \mathcal{P}_i$ is an irredundant prime decomposition of $\sqrt{\text{sat}(\mathcal{B})}$, U is a parametric set of \mathcal{P}_i for each i by [13]. And for prime ideals \mathcal{P}_i , $f \notin \mathcal{P}_i$ if and only if $(f, \mathcal{P}_i) \cap \mathcal{F}[U] \neq \{0\}$. If f is invertible w.r.t. $\text{sat}(\mathcal{B})$, $\{0\} \neq (f, \text{sat}(\mathcal{B})) \cap \mathcal{F}[U] \subset (f, \mathcal{P}_i) \cap \mathcal{F}[U]$. Thus, $f \notin \mathcal{P}_i$ for each i . For the other side, suppose $f \notin \mathcal{P}_i$ for all i , then there exist nonzero polynomials $h_i(U)$ such that $h_i(U) \in (f, \mathcal{P}_i)$. Thus, there exists $t \in \mathbb{N}$ such that $(\prod_{i=1}^m h_i(U))^t \in (f, \text{sat}(\mathcal{B}))$. So f is invertible w.r.t. $\text{sat}(\mathcal{B})$. \square

Lemma 2.5 [2] Let \mathcal{B} be a regular chain in $\mathcal{F}[U, Y]$. Let f be a polynomial in $\mathcal{F}[U, Y]$ and L in $\mathcal{F}[U] \setminus \{0\}$ such that $Lf \in (\mathcal{B})$. Then $f \in \text{sat}(\mathcal{B})$.

Lemma 2.6 Let A be an irreducible difference polynomial in $\mathcal{F}\{\mathbb{Y}\}$ with $\deg(A, y_{i_0}) > 0$ for some i_0 . If f is invertible w.r.t. $A^{[k]} = A, A^{(1)}, \dots, A^{(k)}$ under some ranking \mathcal{R} , then $\sigma(f)$ is invertible w.r.t. $A^{[k+1]} = A, \dots, A^{(k+1)}$. In particular, $A^{[k]}$ is a regular chain for any $k \geq 0$.

Proof: Since as a difference ascending chain, A is coherent and proper irreducible, by Theorem 4.1 in [15], A is difference regular. As a consequence, $A^{[k]}$ is regular for any $k \geq 0$. \square

The following fact is needed to define sparse difference resultant.

Lemma 2.7 *Let \mathcal{I} be a reflexive prime difference ideal of codimension one in $\mathcal{F}\{\mathbb{Y}\}$. The first element in any characteristic set of \mathcal{I} w.r.t. any ranking, when taken irreducible, is unique up to a factor in \mathcal{F} .*

Proof: Let $\mathcal{A} = A_1, \dots, A_m$ be a characteristic set of \mathcal{I} w.r.t. some ranking \mathcal{R} with A_1 irreducible. Suppose $\text{lvar}(\mathcal{A}) = y_1$. Given another characteristic set $\mathcal{B} = B_1, \dots, B_l$ of \mathcal{I} w.r.t. some other ranking \mathcal{R}' (B_1 is irreducible), we need to show that there exists $c \in \mathcal{F}$ such that $B_1 = c \cdot A_1$. It suffices to consider the case $\text{lvar}(\mathcal{B}) \neq y_1$. Suppose $\text{lvar}(B_1) = y_2$. Clearly, y_2 appears effectively in A_1 for \mathcal{B} reduces A_1 to 0. And since \mathcal{I} is reflexive, there exists some i_0 such that $\deg(A_1, y_{i_0}) > 0$.

Suppose $\text{ord}(A_1, y_2) = o_2$. Take another ranking under which $y_2^{(o_2)}$ is the leader of A_1 and we use \tilde{A}_1 to distinguish it from the A_1 under \mathcal{R} . By Lemma 2.6, for each k , $A_1^{[k]}$ and $\tilde{A}_1^{[k]}$ are regular chains.

Now we claim that $\text{asat}(A_1^{[k]}) = \text{asat}(\tilde{A}_1^{[k]})$. On the one hand, for any polynomial $f \in \text{asat}(A_1^{[k]})$, we have $(\prod_{i=0}^k \sigma^i(I_{A_1}))^a f \in (A_1^{[k]})$. Since I_{A_1} is invertible w.r.t. \tilde{A}_1 , by Lemma 2.6, $\sigma^i(I_{A_1})$ is invertible w.r.t. $\tilde{A}_1^{[i]}$. Thus, $(\prod_{i=0}^k \sigma^i(I_{A_1}))^a$ is invertible w.r.t. $\tilde{A}_1^{[k]}$. Denote the parameters of $\tilde{A}_1^{[k]}$ by \tilde{U} . So there exists a nonzero polynomial $h(\tilde{U})$ such that $h(\tilde{U}) \in ((\prod_{i=0}^k \sigma^i(I_{A_1}))^a, \tilde{A}_1^{[k]})$. Thus, $h(\tilde{U})f \in (\tilde{A}_1^{[k]})$. Since $\tilde{A}_1^{[k]}$ is a regular chain, by Lemma 2.5, $f \in \text{asat}(\tilde{A}_1^{[k]})$. So $\text{asat}(A_1^{[k]}) \subseteq \text{asat}(\tilde{A}_1^{[k]})$. Similarly, we can show that $\text{asat}(\tilde{A}_1^{[k]}) \subseteq \text{asat}(A_1^{[k]})$. Thus, $\text{asat}(A_1^{[k]}) = \text{asat}(\tilde{A}_1^{[k]})$.

Suppose $\text{ord}(B_1, y_2) = o'_2$. It is clear that $o_2 \geq o'_2$. We now proceed to show that it is impossible for $o_2 > o'_2$. Suppose the contrary, i.e. $o_2 > o'_2$. Then B_1 is invertible w.r.t. $\text{asat}(\tilde{A}_1^{[k]})$. Suppose $\sqrt{\text{asat}(\tilde{A}_1^{[k]})} = \bigcap_{i=1}^t \mathcal{P}_i$ is an irredundant prime decomposition. By Lemma 2.4, $B_1 \notin \mathcal{P}_i$ for each i . Since $\text{asat}(A_1^{[k]}) = \text{asat}(\tilde{A}_1^{[k]})$, using Lemma 2.4 again, B_1 is invertible w.r.t. $\text{asat}(A_1^{[k]})$. Thus, there exists a nonzero difference polynomial H with $\text{ord}(H, y_1) < \text{ord}(A_1, y_1)$ such that $H \in (B_1, \text{asat}(A_1^{[k]})) \subset \mathcal{I}$, which is a contradiction. Thus, $o_2 = o'_2$. Since \mathcal{B} reduces A_1 to zero and A_1 is irreducible, there exists $c \in \mathcal{F}$ such that $B_1 = c \cdot A_1$. \square

3 Sparse difference resultant

In this section, the concepts of Laurent difference polynomials and transformally essential systems are first introduced, and then the sparse difference resultant for transformally essential systems is defined. And we also give a criterion for Laurent transformally essential systems in terms of the support of the given system.

3.1 Laurent difference polynomial

Let \mathcal{F} be an ordinary difference field with a transforming operator σ and $\mathcal{F}\{\mathbb{Y}\}$ the ring of difference polynomials in the difference indeterminates $\mathbb{Y} = \{y_1, \dots, y_n\}$. Similar to [23], before defining sparse difference resultant, we first introduce the concept of Laurent difference polynomials.

Definition 3.1 *A Laurent difference monomial of order s is a Laurent monomial in variables $\mathbb{Y}^{[s]} = (y_i^{(k)})_{1 \leq i \leq n, 0 \leq k \leq s}$. More precisely, it has the form $\prod_{i=1}^n \prod_{k=0}^s (y_i^{(k)})^{d_{ik}}$ where d_{ik} are integers which can be negative. A Laurent difference polynomial over \mathcal{F} is a finite linear combination of Laurent difference monomials with coefficients in \mathcal{F} .*

Clearly, the collections of all Laurent difference polynomials form a commutative difference ring under the obvious sum, product operations and the usual transforming operator σ , where all Laurent difference monomials are invertible. We denote the difference ring of Laurent difference polynomials with coefficients in \mathcal{F} by $\mathcal{F}\{y_1, y_1^{-1}, \dots, y_n, y_n^{-1}\}$, or simply by $\mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$.

Definition 3.2 *For every Laurent difference polynomial $F \in \mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$, there exists a unique Laurent difference monomial M such that 1) $M \cdot F \in \mathcal{F}\{\mathbb{Y}\}$ and 2) for any Laurent difference monomial T with $T \cdot F \in \mathcal{E}\{\mathbb{Y}\}$, $T \cdot F$ is divisible by $M \cdot F$ as polynomials. This $M \cdot F$ is defined to be the norm form of F , denoted by $N(F)$. The order and degree of $N(F)$ is defined to be the order and degree of F , denoted by $\text{ord}(F)$ and $\text{deg}(F)$.*

In the following, we consider zeros for Laurent difference polynomials.

Definition 3.3 *Let F be a Laurent difference polynomial in $\mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$. An n -tuple (a_1, \dots, a_n) over \mathcal{F} is called a nonzero difference zero of F if for all i , $a_i \neq 0$ and $F(a_1, \dots, a_n) = 0$.*

For an ideal $\mathcal{I} \in \mathcal{F}\{\mathbb{Y}, \mathbb{Y}^{-1}\}$, the difference zero set of \mathcal{I} is the set of common nonzero difference zeros of all Laurent difference polynomials in \mathcal{I} . We will see later in Example 4.2, how nonzero difference solutions are naturally related with the sparse difference resultant.

3.2 Definition of sparse difference resultant

In this section, the definition of the sparse difference resultant will be given. Similar to the study of sparse differential resultants, we first define sparse difference resultants for Laurent difference polynomials whose coefficients are difference indeterminates. Then the sparse difference resultant for a given Laurent difference polynomial system with concrete coefficients is the value which the resultant in the generic case assumes for the given case.

Suppose $\mathcal{A}_i = \{M_{i0}, M_{i1}, \dots, M_{il_i}\}$ ($i = 0, 1, \dots, n$) are finite sets of Laurent difference monomials in \mathbb{Y} . Consider $n + 1$ generic Laurent difference polynomials defined over $\mathcal{A}_0, \dots, \mathcal{A}_n$:

$$\mathbb{P}_i = \sum_{k=0}^{l_i} u_{ik} M_{ik} \quad (i = 0, \dots, n), \quad (1)$$

where all the u_{ik} are transformally independent over the rational number field \mathbb{Q} . Denote

$$\mathbf{u}_i = (u_{i0}, u_{i1}, \dots, u_{in}) \ (i = 0, \dots, n) \text{ and } \mathbf{u} = \cup_{i=0}^n \mathbf{u}_i \setminus \{u_{i0}\}. \quad (2)$$

The number $l_i + 1$ is called the *size* of \mathbb{P}_i . To avoid the triviality, $l_i \geq 1$ ($i = 0, \dots, n$) are always assumed in this paper.

Definition 3.4 *A set of Laurent difference polynomials of form (1) is called Laurent transformally essential if there exist k_i ($i = 0, \dots, n$) with $1 \leq k_i \leq l_i$ such that $\Delta \text{tr.deg } \mathbb{Q}\langle \frac{M_{0k_0}}{M_{00}}, \frac{M_{1k_1}}{M_{10}}, \dots, \frac{M_{nk_n}}{M_{n0}} \rangle / \mathbb{Q} = n$. In this case, we also say that $\mathcal{A}_0, \dots, \mathcal{A}_n$ form a Laurent transformally essential system.*

Although M_{i0} are used as denominators to define transformally essential system, the following lemma shows that the definition does not depend on the choices of M_{i0} .

Lemma 3.5 *The following two conditions are equivalent.*

1. *There exist k_i ($i = 0, \dots, n$) with $1 \leq k_i \leq l_i$ such that $\Delta \text{tr.deg } \mathbb{Q}\langle \frac{M_{0k_0}}{M_{00}}, \dots, \frac{M_{nk_n}}{M_{n0}} \rangle / \mathbb{Q} = n$.*
2. *There exist pairs (k_i, j_i) ($i = 0, \dots, n$) with $k_i \neq j_i \in \{0, \dots, l_i\}$ such that $\Delta \text{tr.deg } \mathbb{Q}\langle \frac{M_{0k_0}}{M_{0j_0}}, \dots, \frac{M_{nk_n}}{M_{nj_n}} \rangle / \mathbb{Q} = n$.*

Proof: Similar to the proof of [23, Lemma 3.7], it can be easily shown. \square

Let \mathfrak{m} be the set of all difference monomials in \mathbb{Y} and $[N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)]$ the difference ideal generated by $N(\mathbb{P}_i)$ in $\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}$. Let

$$\mathcal{I}_{\mathbb{Y}, \mathbf{u}} = ([N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)] : \mathfrak{m}). \quad (3)$$

The following result is a foundation for defining sparse difference resultants.

Theorem 3.6 *Let $\mathbb{P}_0, \dots, \mathbb{P}_n$ be Laurent difference polynomials defined in (1). Then the following assertions hold.*

1. *$\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ is a reflexive prime difference ideal in $\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}$.*
2. *$\mathcal{I}_{\mathbb{Y}, \mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is of codimension one if and only if $\mathbb{P}_0, \dots, \mathbb{P}_n$ form a Laurent transformally essential system.*

Proof: Let $\eta = (\eta_1, \dots, \eta_n)$ be a sequence of transformally independent elements over $\mathbb{Q}\langle \mathbf{u} \rangle$, where \mathbf{u} is defined in (2). Let

$$\zeta_i = - \sum_{k=1}^{l_i} u_{ik} \frac{M_{ik}(\eta)}{M_{i0}(\eta)} \ (i = 0, 1, \dots, n). \quad (4)$$

We claim that $\theta = (\eta; \zeta_0, u_{01}, \dots, u_{0l_0}; \dots; \zeta_n, u_{n1}, \dots, u_{nl_n})$ is a generic point of $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$, which follows that $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ is a reflexive prime difference ideal.

Denote $N(\mathbb{P}_i) = M_i \mathbb{P}_i$ ($i = 0, \dots, n$) where M_i are Laurent difference monomials. Clearly, $N(\mathbb{P}_i) = M_i \mathbb{P}_i$ vanishes at θ ($i = 0, \dots, n$). For any $f \in \mathcal{I}_{\mathbb{Y}, \mathbf{u}}$, there exists an $M \in \mathfrak{m}$ such that $Mf \in [N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)]$. It follows that $f(\theta) = 0$. Conversely, let f be any difference polynomial in $\mathbb{Q}\{\mathbb{Y}, \mathbf{u}_0, \dots, \mathbf{u}_n\}$ satisfying $f(\theta) = 0$. Clearly, $N(\mathbb{P}_0), N(\mathbb{P}_1), \dots, N(\mathbb{P}_n)$ constitute an ascending chain with u_{i0} as leaders. Let f_1 be the difference remainder of f w.r.t. this ascending chain. Then f_1 is free from u_{i0} ($i = 0, \dots, n$) and there exist $a, s \in \mathbb{N}$ such that $(\prod_{i=0}^n \prod_{l=0}^s (\sigma^l(M_i M_{i0})))^a \cdot f \equiv f_1 \pmod{[N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)]}$. Clearly, $f_1(\theta) = 0$. Since $f_1 \in \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\}$, $f_1 = 0$. Thus, $f \in \mathcal{I}_{\mathbb{Y}, \mathbf{u}}$. So $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ is a reflexive prime difference ideal with a generic point θ .

Consequently, $\mathcal{I}_{\mathbb{Y}, \mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is a reflexive prime difference ideal with a generic point $\zeta = (\zeta_0, u_{01}, \dots, u_{0l_0}; \dots; \zeta_n, u_{n1}, \dots, u_{nl_n})$. From (4), it is clear that $\Delta \text{tr.deg } \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} \leq \sum_{i=0}^n l_i + n$. If there exist pairs (i_k, j_k) ($k = 1, \dots, n$) with $1 \leq j_k \leq l_{i_k}$ and $i_{k_1} \neq i_{k_2}$ ($k_1 \neq k_2$) such that $\frac{M_{i_1 j_1}}{M_{i_1 0}}, \dots, \frac{M_{i_n j_n}}{M_{i_n 0}}$ are transformally independent over \mathbb{Q} , then by Lemma 2.2, $\zeta_{i_1}, \dots, \zeta_{i_n}$ are transformally independent over $\mathbb{Q}\langle \mathbf{u} \rangle$. It follows that $\Delta \text{tr.deg } \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} = \sum_{i=0}^n l_i + n$. Thus, $\mathcal{I}_{\mathbb{Y}, \mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is of codimension 1.

Conversely, let us assume that $\mathcal{I}_{\mathbb{Y}, \mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is of codimension 1. That is, $\Delta \text{tr.deg } \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} = \sum_{i=0}^n l_i + n$. We want to show that there exist pairs (i_k, j_k) ($k = 1, \dots, n$) with $1 \leq j_k \leq l_{i_k}$ and $i_{k_1} \neq i_{k_2}$ ($k_1 \neq k_2$) such that $\frac{M_{i_1 j_1}}{M_{i_1 0}}, \dots, \frac{M_{i_n j_n}}{M_{i_n 0}}$ are transformally independent over \mathbb{Q} . Suppose the contrary, i.e., $\frac{M_{i_1 j_1}(\eta)}{M_{i_1 0}(\eta)}, \dots, \frac{M_{i_n j_n}(\eta)}{M_{i_n 0}(\eta)}$ are transformally dependent for any n different i_k and $j_k \in \{1, \dots, l_{i_k}\}$. Since each ζ_{i_k} is a linear combination of $\frac{M_{i_k j_k}(\eta)}{M_{i_k 0}(\eta)}$ ($j_k = 1, \dots, l_{i_k}$), it follows that $\zeta_{i_1}, \dots, \zeta_{i_n}$ are transformally dependent over $\mathbb{Q}\langle \mathbf{u} \rangle$. Thus, we have $\Delta \text{tr.deg } \mathbb{Q}\langle \zeta \rangle / \mathbb{Q} < \sum_{i=0}^n l_i + n$, a contradiction to the hypothesis. \square

Let $[\mathbb{P}_0, \dots, \mathbb{P}_n]$ be the difference ideal in $\mathbb{Q}\{\mathbb{Y}, \mathbb{Y}^{-1}; \mathbf{u}_0, \dots, \mathbf{u}_n\}$ generated by \mathbb{P}_i . Then we have

Corollary 3.7 $[\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is a reflexive prime difference ideal of codimension one if and only if $\{\mathbb{P}_i : i = 0, \dots, n\}$ is a Laurent transformally essential system.

Proof: It is easy to show that $[\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\} = \mathcal{I}_{\mathbb{Y}, \mathbf{u}} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$. And the result is a direct consequence of Theorem 3.6. \square

Now suppose $\{\mathbb{P}_0, \dots, \mathbb{P}_n\}$ is a Laurent transformally essential system. Denote the difference ideal $[\mathbb{P}_0, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ by $\mathcal{I}_{\mathbf{u}}$. Since $\mathcal{I}_{\mathbf{u}}$ is a reflexive prime difference ideal of codimension one, by Lemma 2.7, there exists a unique irreducible difference polynomial $\mathbf{R}(\mathbf{u}; u_{00}, \dots, u_{n0}) = \mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n) \in \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ such that \mathbf{R} can serve as the first polynomial in each characteristic set of $\mathcal{I}_{\mathbf{u}}$ w.r.t. any ranking endowed on $\mathbf{u}_0, \dots, \mathbf{u}_n$. That is, if u_{i0} appears in \mathbf{R} , then among all the difference polynomials in $\mathcal{I}_{\mathbf{u}}$, \mathbf{R} is of minimal order in u_{i0} and of minimal degree with the same order.

Now the definition of sparse difference resultant is given as follows:

Definition 3.8 The above $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n) \in \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ is defined to be the sparse difference resultant of the Laurent transformally essential system $\mathbb{P}_0, \dots, \mathbb{P}_n$, denoted by $\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n}$ or $\text{Res}_{\mathbb{P}_0, \dots, \mathbb{P}_n}$. And when all the \mathcal{A}_i are equal to the same \mathcal{A} , we simply denote it by $\text{Res}_{\mathcal{A}}$.

The following lemma gives another description of sparse difference resultant from the perspective of generic point,

Lemma 3.9 *Let $\zeta_i = -\sum_{k=1}^{l_i} u_{ik} \frac{M_{ik}(\eta)}{M_{i0}(\eta)}$ ($i = 0, 1, \dots, n$) defined as in equation (4), where $\eta = (\eta_1, \dots, \eta_n)$ is a generic point of $[0]$ over $\mathbb{Q}\langle \mathbf{u} \rangle$. Then among all the polynomials in $\mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ vanishing at $(\mathbf{u}; \zeta_0, \dots, \zeta_n)$, $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n) = \mathbf{R}(\mathbf{u}; u_{00}, \dots, u_{n0})$ is of minimal order and degree in each u_{i0} ($i = 0, \dots, n$).*

Proof: It is a direct consequence of Theorem 3.6 and Definition 3.8. \square

Remark 3.10 *From its definition, the sparse difference resultant can be computed as follows. With the characteristic set method given in [15], we can compute a proper irreducible ascending chain \mathcal{A} which is a characteristic set for the difference polynomial system $\{\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_n\}$ under a ranking such that $u_{ij} < y_k$. Then the first difference polynomial in \mathcal{A} is the sparse difference resultant. This algorithm does not have a complexity analysis. In Section 5, we will give a single exponential algorithm to compute the sparse difference resultant.*

We give several examples to show sparse difference resultant.

Example 3.11 *Let $n = 2$ and \mathbb{P}_i has the form*

$$\mathbb{P}_i = u_{i0}y_1^{(2)} + u_{i1}y_1^{(3)} + u_{i2}y_2^{(3)} \quad (i = 0, 1, 2).$$

It is easy to show that $y_1^{(3)}/y_1^{(2)}$ and $y_2^{(3)}/y_1^{(2)}$ are transformally independent over \mathbb{Q} . Thus, $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ form a Laurent transformally essential system. The sparse difference resultant is

$$\mathbf{R} = \text{Res}_{\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2} = \begin{vmatrix} u_{00} & u_{01} & u_{02} \\ u_{10} & u_{11} & u_{12} \\ u_{20} & u_{21} & u_{22} \end{vmatrix}.$$

The following example shows that for a Laurent transformally essential system, its sparse difference resultant may not involve the coefficients of some \mathbb{P}_i .

Example 3.12 *Let $n = 2$ and \mathbb{P}_i has the form*

$$\mathbb{P}_0 = u_{00} + u_{01}y_1y_2, \quad \mathbb{P}_1 = u_{10} + u_{11}y_1^{(1)}y_2^{(1)}, \quad \mathbb{P}_2 = u_{20} + u_{21}y_2.$$

Clearly, $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ form a Laurent transformally essential system. And the sparse difference resultant of $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ is

$$\mathbf{R} = u_{00}^{(1)}u_{11} - u_{01}^{(1)}u_{10},$$

which is free from the coefficients of \mathbb{P}_2 .

The above example can be used to illustrate the difference between the differential and difference cases. If $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$ in Example 3.12 are differential polynomials, then the sparse differential resultant is $u_{01}^2u_{10}u_{20}^2u_{21}^2 - u_{01}u'_{00}u_{11}u_{20}u_{21}^2u'_{20} + u_{00}u'_{01}u_{11}u_{20}u_{21}^2u'_{20} + u_{01}u_{00}u_{11}u_{20}^2(u'_{21})^2 + u_{00}u_{01}u_{11}u_{21}^2(u'_{20})^2 - 2u_{01}u_{00}u_{11}u_{20}u_{21}u'_{20}u'_{21} + u_{01}u'_{00}u_{11}u_{20}^2u'_{21}u_{21} - u_{00}u'_{01}u_{11}u_{21}u'_{21}u_{20}^2$ which contains coefficients of $\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2$.

Remark 3.13 When all the \mathcal{A}_i ($i = 0, \dots, n$) are sets of difference monomials, unless explicitly mentioned, we always consider \mathbb{P}_i as Laurent difference polynomials. But when we regard \mathbb{P}_i as difference polynomials, $\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n}$ is also called the sparse difference resultant of the difference polynomials \mathbb{P}_i and we call \mathbb{P}_i a transformally essential system. In this paper, sometimes we regard \mathbb{P}_i as difference polynomials where we will highlight it.

We now define the sparse difference resultant for any set of specific Laurent difference polynomials over a Laurent transformally essential system. For any finite set \mathcal{A} of Laurent difference monomials, we use $\mathcal{L}(\mathcal{A})$ to denote the set of all Laurent difference polynomials of the form $\sum_{M \in \mathcal{A}} a_M M$ where the a_M are in some difference extension field of \mathbb{Q} . Then $\mathcal{L}(\mathcal{A})$ can be considered as the set of all l -tuples over \mathbb{Q} where $l = |\mathcal{A}|$.

Definition 3.14 Let $\mathcal{A}_i = \{M_{i0}, M_{i1}, \dots, M_{il_i}\}$ ($i = 0, 1, \dots, n$) be a Laurent transformally essential system. Consider $n + 1$ Laurent difference polynomials $(F_0, F_1, \dots, F_n) \in \prod_{i=0}^n \mathcal{L}(\mathcal{A}_i)$. The sparse difference resultant of F_0, F_1, \dots, F_n , denoted as $\text{Res}_{F_0, \dots, F_n}$, is obtained by replacing \mathbf{u}_i by the corresponding coefficient vector of F_i in $\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n}(\mathbf{u}_0, \dots, \mathbf{u}_n)$.

A major unsolved problem about difference resultant is whether \mathbf{R} defined above contains all the information about the elimination ideal $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ defined in (3). More precisely, we propose the following problem.

Problem 3.15 As shown by Example 2.3, the characteristic set for a reflexive prime difference ideal could contain more than one elements. Let $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ be the ideal defined in (3). Then $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$ is a reflexive prime difference ideal of codimension one and

$$\mathcal{I}_{\mathbb{Y}, \mathbf{u}} = \text{sat}(\mathbf{R}, R_1, \dots, R_m),$$

where \mathbf{R} is the sparse difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$ and $\mathbf{R}, R_1, \dots, R_m$ is a characteristic set of $\mathcal{I}_{\mathbb{Y}, \mathbf{u}}$. We conjecture that $m = 0$, or equivalently $\mathcal{I}_{\mathbb{Y}, \mathbf{u}} = \text{sat}(\mathbf{R})$, which is similar the differential case. If this is valid, then better properties can be shown for sparse difference resultant as we will explain later.

3.3 Criterion for Laurent transformally essential systems in terms of the supports

Let \mathcal{A}_i ($i = 0, \dots, n$) be finite sets of Laurent difference monomials. According to Definition 3.4, in order to check whether they form a Laurent transformally essential system, we need to check whether there exist $M_{ik_i}, M_{ij_i} \in \mathcal{A}_i$ ($i = 0, \dots, n$) such that $\Delta \text{tr.deg } \mathbb{Q}\langle M_{0k_0}/M_{0j_0}, \dots, M_{nk_n}/M_{nj_n} \rangle / \mathbb{Q} = n$. This can be done with the difference characteristic set method via symbolic computation [15]. In this section, a criterion will be given to check whether a Laurent difference system is essential in terms of their supports, which is conceptually and computationally simpler than the naive approach based on the characteristic set method.

Let $B_i = \prod_{j=1}^n \prod_{k \geq 0}^s (y_j^{(k)})^{d_{ijk}}$ ($i = 1, \dots, m$) be m Laurent difference monomials. We now introduce a new algebraic indeterminate x and let

$$d_{ij} = \sum_{k=0}^s d_{ijk} x^k \quad (i = 1, \dots, m, j = 1, \dots, n)$$

be univariate polynomials in $\mathbb{Z}[x]$. If $\text{ord}(B_i, y_j) = -\infty$, then set $d_{ij} = 0$. The vector $(d_{i1}, d_{i2}, \dots, d_{in})$ is called the *symbolic support vector* of B_i . The matrix $M = (d_{ij})_{m \times n}$ is called the *symbolic support matrix* of B_1, \dots, B_m .

Note that there is a one-to-one correspondence between Laurent difference monomials and their symbolic support vectors, so we will not distinguish these two concepts in case there is no confusion. The same is true for a set of Laurent difference monomials and its symbolic support matrix.

Definition 3.16 A matrix $M = (d_{ij})_{m \times n}$ over $\mathbb{Q}(x)$ is called normal upper-triangular of rank r if for each $i \leq r$, $d_{ii} \neq 0$ and $d_{i,i-k} = 0$ ($1 \leq k \leq i-1$), and the last $m-r$ rows are zero vectors.

A normal upper-triangular matrix is of the following form:

$$\begin{pmatrix} a_{11} & * & \cdots & * & \cdots & * \\ 0 & a_{22} & \cdots & * & \cdots & * \\ \vdots & \vdots & \ddots & & & \vdots \\ 0 & 0 & \cdots & a_{rr} & \cdots & * \\ 0 & 0 & \cdots & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 \end{pmatrix}$$

Definition 3.17 A set of Laurent difference monomials B_1, B_2, \dots, B_m is said to be in r -upper-triangular form if its symbolic support matrix M is a normal upper triangular matrix of rank r .

The following lemma shows that it is easy to compute the difference transcendence degree of a set of Laurent difference monomials in upper-triangular form.

Lemma 3.18 Let B_1, \dots, B_m be a set of Laurent difference monomials in r -upper-triangular form. Then $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_m \rangle / \mathbb{Q} = r$.

Proof: From the structure of the symbolic support matrix, for $i = 1, \dots, r$, $B_i = \prod_{j=i}^n \prod_{k \geq 0} (y_j^{(k)})^{d_{ijk}}$ with $\text{ord}(B_i, y_i) \geq 0$ and $B_{r+1} = \cdots = B_m = 1$. Let $B'_i = \prod_{j=i}^r \prod_{k \geq 0} (y_j^{(k)})^{d_{ijk}}$. Then

$$\begin{aligned} & \Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_m \rangle / \mathbb{Q} \\ &= \Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_r \rangle / \mathbb{Q} \\ &\geq \Delta \text{tr.deg } \mathbb{Q}\langle y_{r+1}, \dots, y_n \rangle \langle B_1, \dots, B_r \rangle / \mathbb{Q} \langle y_{r+1}, \dots, y_n \rangle \\ &= \Delta \text{tr.deg } \mathbb{Q}\langle B'_1, \dots, B'_r \rangle / \mathbb{Q}. \end{aligned}$$

So it suffices to prove $\Delta \text{tr.deg } \mathbb{Q}\langle B'_1, \dots, B'_r \rangle / \mathbb{Q} = r$.

If $r = 1$, B'_1 is a nonconstant Laurent difference monomial in y_1 , so $\Delta \text{tr.deg } \mathbb{Q}\langle B'_1 \rangle / \mathbb{Q} = 1$. Suppose we have proved for the case $r-1$. Let $B''_i = \prod_{j=i}^{r-1} \prod_{k \geq 0} (y_j^{(k)})^{d_{ijk}}$, then by the

hypothesis, $\Delta \text{tr.deg } \mathbb{Q}\langle B_1'', \dots, B_{r-1}'' \rangle / \mathbb{Q} = r - 1$. Thus,

$$\begin{aligned}
r &\geq \Delta \text{tr.deg } \mathbb{Q}\langle B_1', \dots, B_r' \rangle / \mathbb{Q} \\
&= \Delta \text{tr.deg } \mathbb{Q}\langle B_r' \rangle / \mathbb{Q} + \Delta \text{tr.deg } \mathbb{Q}\langle B_1', \dots, B_{r-1}' \rangle / \mathbb{Q}\langle B_r' \rangle \\
&\geq 1 + \Delta \text{tr.deg } \mathbb{Q}\langle y_r \rangle \langle B_1', \dots, B_{r-1}' \rangle / \mathbb{Q}\langle y_r \rangle \\
&= 1 + \Delta \text{tr.deg } \mathbb{Q}\langle B_1'', \dots, B_{r-1}'' \rangle / \mathbb{Q} = r.
\end{aligned}$$

So $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_m \rangle / \mathbb{Q} = r$. \square

In the following, we will show that each set of Laurent difference monomials can be transformed to an upper-triangular set with the same difference transcendence degree. Here we use three types of elementary matrix transformations. For a matrix M over $\mathbb{Q}[x]$, Type 1 operations consist of interchanging two rows of M , say the i -th and j -th rows, denoted by $r[i, j]$; Type 2 operations consist of adding an $f(x)$ -multiple of the j -th row to the i -th row, where $f(x) \in \mathbb{Q}[x]$, denoted by $[i + j(f(x))]$; and Type 3 operations consist of interchanging two columns, say the i -th and j -th columns, denoted by $c[i, j]$. In this section, by elementary transformations, we mean the above three types of transformations.

Let B_1, \dots, B_m be Laurent differential monomials and M their symbolic support matrix. Then the above three types of elementary transformations of M correspond to certain transformations of the difference monomials. Indeed, interchanging the i -th and the j -th rows of M means interchanging B_i and B_j , and interchanging the i -th and the j -th columns of M means interchanging y_i and y_j in B_1, \dots, B_m (or in the variable order). Multiplying the i -th row of M by a polynomial $f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_0 \in \mathbb{Q}[x]$ and adding the result to the j -th row means changing B_j to $\prod_{k=0}^d (\sigma^k B_i)^{a_k} B_j$.

Lemma 3.19 *Let B_1, \dots, B_m be Laurent difference monomials and C_1, \dots, C_m obtained by successive elementary transformations defined above. Then $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_m \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle C_1, \dots, C_m \rangle / \mathbb{Q}$.*

Proof: It suffices to show that Type 2 operations keep the difference transcendence degree. That is, for $\sum_{i=0}^d a_i x^i \in \mathbb{Q}[x]$, $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, B_2 \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle B_1, \prod_{k=0}^d (\sigma^k B_1)^{a_k} B_2 \rangle / \mathbb{Q}$.

Suppose $a_i = p_i/q$ where $p_i, q \in \mathbb{Z}^*$. Then, clearly, $\Delta \text{tr.deg } \mathbb{Q}\langle B_1 \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle \prod_{k=0}^d (\sigma^k B_1)^{p_k} \rangle / \mathbb{Q}$. Thus, $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, \prod_{k=0}^d (\sigma^k B_1)^{a_k} B_2 \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle \prod_{k=0}^d (\sigma^k B_1)^{p_k}, \prod_{k=0}^d (\sigma^k B_1)^{p_k} B_2^q \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle \prod_{k=0}^d (\sigma^k B_1)^{p_k}, B_2^q \rangle / \mathbb{Q} = \Delta \text{tr.deg } \mathbb{Q}\langle B_1, B_2 \rangle / \mathbb{Q}$. \square

Theorem 3.20 *Let B_1, \dots, B_m be a set of Laurent difference monomials with symbolic support matrix M . Then $\Delta \text{tr.deg } \mathbb{Q}\langle B_1, \dots, B_m \rangle / \mathbb{Q} = \text{rk}(M)$.*

Proof: By Lemma 3.18 and Lemma 3.19, it suffices to show that M can be reduced to a normal upper-triangular matrix by performing a series of elementary transformations.

Suppose $M = (d_{ij}) \neq \mathbf{0}_{m \times n}$ and we denote the new matrix obtained after performing elementary transformations also by M . Firstly, perform Type 1 and Type 3 operations when necessary to make $d_{11} \neq 0$. Secondly, try to use $d_{11}(x)$ to reduce other elements in the first column to 0 by performing Type 2 operations. If there exists an element in the first column such that it can not be divisible by d_{11} , say d_{k1} , suppose $d_{k1}(x) = d_{11}(x)q(x) + r(x)$ where $r(x) \neq 0$ and $\deg(r(x)) < \deg(d_{11}(x))$. After performing the transformations $[k + 1(-q(x))]$

and $r[1, k]$ successively, we obtain a new matrix in which the degree of d_{11} strictly decreases. Repeat this process when necessary, then after a finite number of steps, we obtain a new matrix M such that $d_{11}(x)$ divides each nonzero element in the first column, and by using $d_{11}(x)$ to perform Type 2 operations we obtain

$$M = \begin{pmatrix} d_{11} & * \\ \mathbf{0} & M_1 \end{pmatrix}.$$

Now we repeat the above process for M_1 and whenever Type 3 operations are performed for M_1 , we assume the same transformations are performed for the whole matrix M . In this way, after a finite number of steps, we obtain a normal upper-triangular matrix M . \square

Example 3.21 Let $B_1 = y_1 y_2$ and $B_2 = y_1^{(a)} y_2^{(b)}$. Then the symbolic support matrix of B_1 and B_2 is $M = \begin{pmatrix} 1 & 1 \\ x^a & x^b \end{pmatrix}$. Then $\text{rk}(M) = \begin{cases} 1 & \text{if } a = b \\ 2 & \text{if } a \neq b. \end{cases}$ Thus, by Theorem 3.20, if $a \neq b$, B_1 and B_2 are transformally independent over \mathbb{Q} . Otherwise, they are transformally dependent over \mathbb{Q} .

Consider the set of generic Laurent difference polynomials defined in (1):

$$\mathbb{P}_i = u_{i0} M_{i0} + \sum_{k=1}^{l_i} u_{ik} M_{ik} \quad (i = 1, \dots, m).$$

Let β_{ik} be the symbolic support vector of M_{ik}/M_{i0} . Then the vector $w_i = \sum_{k=0}^{l_i} u_{ik} \beta_{ik}$ is called the *symbolic support vector* of \mathbb{P}_i and the matrix $M_{\mathbb{P}}$ whose rows are w_0, \dots, w_n is called the *symbolic support matrix* of $\mathbb{P}_0, \dots, \mathbb{P}_n$. In terms of $M_{\mathbb{P}}$, we have the following result.

Theorem 3.22 Follow the above notations. Then the following three conditions are equivalent.

1. $\mathbb{P}_0, \dots, \mathbb{P}_n$ form a Laurent transformally essential system.
2. There exist M_{ik_i} ($i = 0, \dots, n$) with $1 \leq k_i \leq l_i$ such that the symbolic support matrix of $M_{0k_0}/M_{00}, \dots, M_{nk_n}/M_{n0}$ is of rank n .
3. The rank of $M_{\mathbb{P}}$ is equal to n .

Proof: The equivalence of 1) and 2) is a direct consequence of Theorem 3.20 and Definition 3.4. And the equivalence of 2) and 3) follows from the fact that $\det(M_{\mathbb{P}, \hat{i}}) = \sum_{k_0, \dots, \hat{k}_i, \dots, k_n} \prod_{j=0, j \neq i}^n u_{jk_j} \det((\beta_{0k_0}, \dots, \hat{\beta}_{ik_i}, \dots, \beta_{nk_n})^T)$, where $M_{\mathbb{P}, \hat{i}}$ is the matrix obtained by deleting the $(i+1)$ -th row from M . \square

We will end this section by introducing a new concept, namely super-essential systems, through which one can identify certain \mathbb{P}_i such that their coefficients will not occur in the sparse difference resultant. This will lead to the simplification in the computation of the resultant. Let $\mathbb{T} \subset \{0, 1, \dots, n\}$. We denote by $\mathbb{P}_{\mathbb{T}}$ the Laurent difference polynomial set consisting of \mathbb{P}_i ($i \in \mathbb{T}$), and $M_{\mathbb{P}_{\mathbb{T}}}$ its symbolic support matrix. For a subset $\mathbb{T} \subset \{0, 1, \dots, n\}$, if $\text{card}(\mathbb{T}) = \text{rk}(M_{\mathbb{P}_{\mathbb{T}}})$, then $\mathbb{P}_{\mathbb{T}}$, or $\{\mathcal{A}_i : i \in \mathbb{T}\}$, is called a *transformally independent set*.

Definition 3.23 Let $\mathbb{T} \subset \{0, 1, \dots, n\}$. Then we call \mathbb{T} or $\mathbb{P}_{\mathbb{T}}$ super-essential if the following conditions hold: (1) $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) = 1$ and (2) $\text{card}(\mathbb{J}) = \text{rk}(M_{\mathbb{P}_{\mathbb{J}}})$ for each proper subset \mathbb{J} of \mathbb{T} .

Note that super-essential systems are the difference analogue of essential systems introduced in [27] and also that of rank essential systems introduced in [23]. Using this definition, we have the following property, which is similar to Corollary 1.1 in [27].

Theorem 3.24 If $\{\mathbb{P}_0, \dots, \mathbb{P}_n\}$ is a Laurent transformally essential system, then for any $\mathbb{T} \subset \{0, 1, \dots, n\}$, $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) \leq 1$ and there exists a unique \mathbb{T} which is super-essential. In this case, the sparse difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$ involves only the coefficients of \mathbb{P}_i ($i \in \mathbb{T}$).

Proof: Since $n = \text{rk}(M_{\mathbb{P}}) \leq \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) + \text{card}(\mathbb{P}) - \text{card}(\mathbb{P}_{\mathbb{T}}) = n + 1 + \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) - \text{card}(\mathbb{T})$, we have $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) \leq 1$. Since $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) \geq 0$, for any \mathbb{T} , either $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) = 0$ or $\text{card}(\mathbb{T}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}}}) = 1$. From this fact, it is easy to show the existence of a super-essential set \mathbb{T} . For the uniqueness, we assume that there exist two subsets $\mathbb{T}_1, \mathbb{T}_2 \subset \{1, \dots, m\}$ which are super-essential. Then, we have

$$\begin{aligned} \text{rk}(M_{\mathbb{P}_{\mathbb{T}_1 \cup \mathbb{T}_2}}) &\leq \text{rk}(M_{\mathbb{P}_{\mathbb{T}_1}}) + \text{rk}(M_{\mathbb{P}_{\mathbb{T}_2}}) - \text{rk}(M_{\mathbb{P}_{\mathbb{T}_1 \cap \mathbb{T}_2}}) \\ &= \text{card}(\mathbb{T}_1) - 1 + \text{card}(\mathbb{T}_2) - 1 - \text{card}(\mathbb{T}_1 \cap \mathbb{T}_2) \\ &= \text{card}(\mathbb{T}_1 \cup \mathbb{T}_2) - 2, \end{aligned}$$

which means that $M_{\mathbb{P}}$ is not of full rank, a contradiction.

Let \mathbb{T} be a super-essential set. Similar to the proof of Theorem 3.6, it is easy to show that $[\mathbb{P}_i]_{i \in \mathbb{T}} \cap \mathbb{Q}\{\mathbf{u}_i\}_{i \in \mathbb{T}}$ is of codimension one, which means that the sparse difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$ involves only of coefficients of \mathbb{P}_i ($i \in \mathbb{T}$). \square

Using this property, one can determine which polynomial is needed for computing the sparse difference resultant, which will eventually reduce the computation complexity.

Example 3.25 Continue from Example 3.12. It is easy to show that $\mathbb{P} = \{\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2\}$ is a Laurent transformally essential system and $\mathbb{P}_0, \mathbb{P}_1$ constitute a super-essential system. Recall that the sparse difference resultant of \mathbb{P} is free from the coefficients of \mathbb{P}_2 .

4 Basic properties of sparse difference resultant

In this section, we will prove some basic properties for the sparse difference resultant $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$.

4.1 Necessary condition for existence of nonzero solutions

In this section, we will first give a condition for a system of Laurent difference polynomials to have nonzero solutions in terms of sparse difference resultant, and then study the structures of nonzero solutions.

To be more precise, we first introduce some notations. Let $\mathcal{A}_0, \dots, \mathcal{A}_n$ be a Laurent transformally essential system of Laurent monomial sets. Each element $(F_0, \dots, F_n) \in \mathcal{L}(\mathcal{A}_0) \times$

$\cdots \times \mathcal{L}(\mathcal{A}_n)$ can be represented by one and only one point $(\mathbf{v}_0, \dots, \mathbf{v}_n) \in \mathcal{E}^{l_0+1} \times \cdots \times \mathcal{E}^{l_n+1}$ where $\mathbf{v}_i = (v_{i0}, v_{i1}, \dots, v_{il_i})$ is the coefficient vector of F_i and \mathcal{E} is some difference field extension of \mathbb{Q} (\mathcal{E} is not fixed but depends on the set F_i). Let $Z_0(\mathcal{A}_0, \dots, \mathcal{A}_n)$ be a set consisting of points $(\mathbf{v}_0, \dots, \mathbf{v}_n)$ such that the corresponding $F_i = 0$ ($i = 0, \dots, n$) have nonzero solutions. That is,

$$Z_0(\mathcal{A}_0, \dots, \mathcal{A}_n) = \{(\mathbf{v}_0, \dots, \mathbf{v}_n) : F_0 = \cdots = F_n = 0 \text{ have a common nonzero solution}\}. \quad (5)$$

The following result shows that the vanishing of sparse differential resultant gives a necessary condition for the existence of nonzero solutions.

Lemma 4.1 $Z_0(\mathcal{A}_0, \dots, \mathcal{A}_n) \subseteq \mathbb{V}(\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n})$.

Proof: Let $\mathbb{P}_0, \dots, \mathbb{P}_n$ be a generic Laurent transformally essential system corresponding to $\mathcal{A}_0, \dots, \mathcal{A}_n$ with coefficient vectors $\mathbf{u}_0, \dots, \mathbf{u}_n$. By Definition 3.8, $\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n} \in [\mathbb{P}_0, \mathbb{P}_1, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$. For any point $(\mathbf{v}_0, \dots, \mathbf{v}_n) \in Z_0(\mathcal{A}_0, \dots, \mathcal{A}_n)$, let $(\overline{\mathbb{P}}_0, \dots, \overline{\mathbb{P}}_n) \in \mathcal{L}(\mathcal{A}_0) \times \cdots \times \mathcal{L}(\mathcal{A}_n)$ be the difference polynomial system represented by $(\mathbf{v}_0, \dots, \mathbf{v}_n)$. Since $\overline{\mathbb{P}}_0, \dots, \overline{\mathbb{P}}_n$ have a nonzero common solution, $\text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n}$ vanishes at $(\mathbf{v}_0, \dots, \mathbf{v}_n)$. \square

Example 4.2 *Continue from Example 3.11. Suppose $\mathcal{F} = \mathbb{Q}(x)$ and $\sigma f(x) = f(x+1)$. In this example, we have $\text{Res}_{\mathbb{P}_0, \mathbb{P}_1, \mathbb{P}_2} \neq 0$. But $y_1 = 0, y_2 = 0$ consist of a zero solution of $\mathbb{P}_0 = \mathbb{P}_1 = \mathbb{P}_2 = 0$. This shows that Lemma 4.1 is not correct if we do not consider nonzero solutions. This example also shows why we need to consider nonzero difference solutions, or equivalently why we consider Laurent difference polynomials instead of usual difference polynomials.*

Remark 4.3 *If Problem 3.15 can be solved positively, then $\mathbf{R} = 0$ also gives a sufficient condition for $\mathbb{P}_0 = \cdots = \mathbb{P}_n = 0$ to have a nonzero solution in certain sense.*

The following lemma reflects the structures of the nonzero solutions.

Lemma 4.4 *Let $\mathcal{A}_0, \dots, \mathcal{A}_n$ be a Laurent transformally essential system and $\mathbf{R} = \text{Res}_{\mathcal{A}_0, \dots, \mathcal{A}_n}$. Then there exists some τ such that $\deg(\mathbf{R}, u_{\tau 0}) > 0$. Suppose $\overline{\mathbb{P}}_i = 0$ is a system represented by $(\mathbf{v}_0, \dots, \mathbf{v}_n) \in Z_0(\mathcal{A}_0, \dots, \mathcal{A}_n)$ and $\frac{\partial \mathbf{R}}{\partial u_{\tau 0}}(\mathbf{v}_0, \dots, \mathbf{v}_n) \neq 0$. If ξ is a common nonzero difference solution of $\overline{\mathbb{P}}_i = 0$ ($i = 0, \dots, n$), then for each k , we have*

$$\frac{M_{\tau k}(\xi)}{M_{\tau 0}(\xi)} = \frac{\partial \mathbf{R}}{\partial u_{\tau k}}(\mathbf{v}_0, \dots, \mathbf{v}_n) \Big/ \frac{\partial \mathbf{R}}{\partial u_{\tau 0}}(\mathbf{v}_0, \dots, \mathbf{v}_n). \quad (6)$$

Proof: Since $\mathcal{I} = [\mathbb{N}(\mathbb{P}_0), \dots, \mathbb{N}(\mathbb{P}_n)] : \mathfrak{m}$ is a reflexive prime difference ideal and $\mathbf{R} \in \mathcal{I}$, there exists some τ and k such that $\deg(\mathbf{R}, u_{\tau k}) > 0$. By Lemma 4.8, $\deg(\mathbf{R}, u_{\tau 0}) > 0$. Denote $\mathbb{N}(\mathbb{P}_i) = M_i \mathbb{P}_i$ ($i = 0, \dots, n$). For each $j = 1, \dots, l_0$, by equation (7) with $k = 0$, the polynomial $\frac{\partial \mathbf{R}}{\partial u_{\tau 0}} M_{\tau} M_{\tau j} - \frac{\partial \mathbf{R}}{\partial u_{\tau j}} M_{\tau} M_{\tau 0} \in \mathcal{I}$. Thus, if ξ is a common nonzero difference solution of $\overline{\mathbb{P}}_i = 0$, then $\frac{\partial \mathbf{R}}{\partial u_{\tau 0}}(\mathbf{v}_0, \dots, \mathbf{v}_n) \cdot M_{\tau j}(\xi) - \frac{\partial \mathbf{R}}{\partial u_{\tau j}}(\mathbf{v}_0, \dots, \mathbf{v}_n) M_{\tau 0}(\xi) = 0$. Since $\frac{\partial \mathbf{R}}{\partial u_{\tau 0}}(\mathbf{v}_0, \dots, \mathbf{v}_n) \neq 0$, (6) follows. \square

4.2 Sparse difference resultant is transformally homogeneous

We now introduce the concept of transformally homogeneous polynomials.

Definition 4.5 A difference polynomial $f \in \mathcal{F}\{y_0, \dots, y_n\}$ is called transformally homogeneous if for a new difference indeterminate λ , there exists a difference monomial $M(\lambda)$ in λ such that $f(\lambda y_0, \dots, \lambda y_n) = M(\lambda)p(y_0, \dots, y_n)$. If $\deg(M(\lambda)) = m$, f is called transformally homogeneous of degree m .

The difference analogue of Euler's theorem related to homogeneous polynomials is valid.

Lemma 4.6 $f \in \mathcal{F}\{y_0, y_1, \dots, y_n\}$ is transformally homogeneous if and only if for each $r \in \mathbb{N}_0$, there exists $m_r \in \mathbb{N}_0$ such that

$$\sum_{i=0}^n y_i^{(r)} \frac{\partial f(y_0, \dots, y_n)}{\partial y_i^{(r)}} = m_r f.$$

Proof: “ \implies ” Denote $\mathbb{Y} = (y_0, \dots, y_n)$ temporarily. Suppose f is transformally homogeneous. That is, there exists a difference monomial $M(\lambda) = \prod_{r=0}^{r_0} (\lambda^{(r)})^{m_r}$ such that $f(\lambda \mathbb{Y}) = M(\lambda)f(\mathbb{Y})$. Then $\sum_{i=0}^n y_i^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda \mathbb{Y}) = \sum_{i=0}^n \frac{\partial f}{\partial y_i^{(r)}}(\lambda \mathbb{Y}) \frac{\partial(\lambda y_i)^{(r)}}{\partial \lambda^{(r)}} = \frac{\partial f(\lambda \mathbb{Y})}{\partial \lambda^{(r)}} = \frac{\partial M(\lambda)f(\mathbb{Y})}{\partial \lambda^{(r)}} = \frac{m_r}{\lambda^{(r)}} f(\lambda \mathbb{Y})$. Substitute $\lambda = 1$ into the above equality, we have $\sum_{i=0}^n y_i^{(r)} \frac{\partial f}{\partial y_i^{(r)}} = m_r f$.

“ \impliedby ” Suppose $\text{ord}(f, \mathbb{Y}) = r_0$. Then for each $r \leq r_0$, $\lambda^{(r)} \frac{\partial f(\lambda \mathbb{Y})}{\partial \lambda^{(r)}} = \lambda^{(r)} \sum_{i=0}^n y_i^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda \mathbb{Y}) = \sum_{i=0}^n (\lambda y_i)^{(r)} \frac{\partial f}{\partial y_i^{(r)}}(\lambda \mathbb{Y}) = m_r f(\lambda \mathbb{Y})$. So $f(\lambda \mathbb{Y})$ is homogeneous of degree m_r in $\lambda^{(r)}$. Thus, $f(\lambda \mathbb{Y}) = f(\lambda y_0, \dots, \lambda y_n; \lambda^{(1)} y_0^{(1)}, \dots, \lambda^{(1)} y_n^{(1)}; \dots; \lambda^{(r_0)} y_0^{(r_0)}, \dots, \lambda^{(r_0)} y_n^{(r_0)}) = \prod_{r=0}^{r_0} (\lambda^{(r)})^{m_r} f(\mathbb{Y})$. Thus, f is transformally homogeneous. \square

Sparse difference resultants have the following property.

Theorem 4.7 The sparse difference resultant is transformally homogeneous in each \mathbf{u}_i which is the coefficient set of \mathbb{P}_i .

Proof: Suppose $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \geq 0$. Follow the notations used in Theorem 3.6. By Lemma 3.9, $\mathbf{R}(\mathbf{u}; \zeta_0, \dots, \zeta_n) = 0$. Differentiating this identity w.r.t. $u_{ij}^{(k)}$ ($j = 1, \dots, l_i$) respectively, we have

$$\frac{\overline{\partial \mathbf{R}}}{\partial u_{ij}^{(k)}} + \frac{\overline{\partial \mathbf{R}}}{\partial u_{i0}^{(k)}} \left(-\frac{M_{ij}(\eta)}{M_{i0}(\eta)} \right)^{(k)} = 0. \quad (7)$$

In the above equations, $\frac{\overline{\partial \mathbf{R}}}{\partial u_{ij}^{(k)}} (k = 0, \dots, h_i; j = 0, \dots, l_i)$ are obtained by replacing u_{i0} by $\zeta_i (i = 0, 1, \dots, n)$ in each $\frac{\overline{\partial \mathbf{R}}}{\partial u_{ij}^{(k)}}$ respectively.

Multiplying (7) by $u_{ij}^{(k)}$ and for j from 1 to l_i , adding them together, we get $\sum_{j=1}^{l_i} u_{ij}^{(k)} \frac{\overline{\partial \mathbf{R}}}{\partial u_{ij}^{(k)}} + \frac{\overline{\partial \mathbf{R}}}{\partial u_{i0}^{(k)}} \zeta_i^{(k)} = 0$. Thus, the difference polynomial $f_k = \sum_{j=0}^{l_i} u_{ij}^{(k)} \frac{\overline{\partial \mathbf{R}}}{\partial u_{ij}^{(k)}}$ vanishes at $(\zeta_0, \dots, \zeta_n)$.

Since $\text{ord}(f_k, u_{i0}) \leq \text{ord}(\mathbf{R}, u_{i0})$ and $\deg(f_k) = \deg(\mathbf{R})$, by Lemma 3.9, there exists an $m_k \in \mathbb{Z}$ such that $f_k = m_k \mathbf{R}$. Thus, by Lemma 4.6, \mathbf{R} is transformally homogeneous in \mathbf{u}_i . \square

4.3 Order bound in terms of Jacobi number

In this section, we will give an order bound for the sparse difference resultant in terms of the Jacobi number of the given system similar to the differential case.

Consider a generic Laurent transformally essential system $\{\mathbb{P}_0, \dots, \mathbb{P}_n\}$ defined in (1) with $\mathbf{u}_i = (u_{i0}, u_{i1}, \dots, u_{il_i})$ being the coefficient vector of \mathbb{P}_i ($i = 0, \dots, n$). Suppose \mathbf{R} is the sparse difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$. Denote $\text{ord}(\mathbf{R}, \mathbf{u}_i)$ to be the maximal order of \mathbf{R} in u_{ik} ($k = 0, \dots, l_i$), that is, $\text{ord}(\mathbf{R}, \mathbf{u}_i) = \max_k \text{ord}(\mathbf{R}, u_{ik})$. If \mathbf{u}_i does not occur in \mathbf{R} , then set $\text{ord}(\mathbf{R}, \mathbf{u}_i) = -\infty$. Firstly, we have the following result.

Lemma 4.8 *For fixed i and s , if there exists k_0 such that $\deg(\mathbf{R}, u_{ik_0}^{(s)}) > 0$, then for all $k \in \{0, 1, \dots, l_i\}$, $\deg(\mathbf{R}, u_{ik}^{(s)}) > 0$. In particular, if $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \geq 0$, then $\text{ord}(\mathbf{R}, u_{ik}) = h_i$ ($k = 0, \dots, l_i$).*

Proof: Firstly, for each $k \in \{1, \dots, l_i\}$, by differentiating $\mathbf{R}(\mathbf{u}; \zeta_0, \dots, \zeta_n) = 0$ w.r.t. $u_{ik}^{(s)}$, we have $\frac{\partial \mathbf{R}}{\partial u_{ik}^{(s)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) + \frac{\partial \mathbf{R}}{\partial u_{i0}^{(s)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) \left(-\frac{M_{ik}(\eta)}{M_{i0}(\eta)} \right)^{(s)} = 0$. If $k_0 = 0$, then $\frac{\partial \mathbf{R}}{\partial u_{i0}^{(s)}}$ is a nonzero difference polynomial not vanishing at $(\mathbf{u}, \zeta_0, \dots, \zeta_n)$ by lemma 3.9. So $\frac{\partial \mathbf{R}}{\partial u_{ik}^{(s)}} \neq 0$. Thus, $\deg(\mathbf{R}, u_{ik}^{(s)}) > 0$ for each k . If $k_0 \neq 0$, then $\frac{\partial \mathbf{R}}{\partial u_{ik_0}^{(s)}}(\mathbf{u}, \zeta_0, \dots, \zeta_n) \neq 0$ and $\frac{\partial \mathbf{R}}{\partial u_{i0}^{(s)}} \neq 0$ follows. So by the case $k_0 = 0$, for all k , $\deg(\mathbf{R}, u_{ik}^{(s)}) > 0$.

In particular, if $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i \geq 0$, then there exists some k_0 such that $\deg(\mathbf{R}, u_{ik_0}^{(h_i)}) > 0$. Thus, for each $k = 0, \dots, l_i$, $\deg(\mathbf{R}, u_{ik}^{(h_i)}) > 0$ and $\text{ord}(\mathbf{R}, u_{ik}) = h_i$ follows. \square

Let $A = (a_{ij})$ be an $n \times n$ matrix where a_{ij} is an integer or $-\infty$. A *diagonal sum* of A is any sum $a_{1\sigma(1)} + a_{2\sigma(2)} + \dots + a_{n\sigma(n)}$ with σ a permutation of $1, \dots, n$. If A is an $m \times n$ matrix with $M = \min\{m, n\}$, then a diagonal sum of A is a diagonal sum of any $M \times M$ submatrix of A . The *Jacobi number* of a matrix A is the maximal diagonal sum of A , denoted by $\text{Jac}(A)$.

Let $\text{ord}(\mathbf{N}(\mathbb{P}_i), y_j) = s_{ij}$ ($i = 0, \dots, n; j = 1, \dots, n$) and $\text{ord}(\mathbf{N}(\mathbb{P}_i)) = s_i$. We call the $(n+1) \times n$ matrix $A = (s_{ij})$ the *order matrix* of $\mathbb{P}_0, \dots, \mathbb{P}_n$. By A_i , we mean the submatrix of A obtained by deleting the $(i+1)$ -th row from A . We use \mathbb{P} to denote the set $\{\mathbf{N}(\mathbb{P}_0), \dots, \mathbf{N}(\mathbb{P}_n)\}$ and by \mathbb{P}_i , we mean the set $\mathbb{P} \setminus \{\mathbf{N}(\mathbb{P}_i)\}$. We call $J_i = \text{Jac}(A_i)$ the *Jacobi number* of the system \mathbb{P}_i , also denoted by $\text{Jac}(\mathbb{P}_i)$. Before giving an order bound for sparse difference resultant in terms of the Jacobi numbers, we first list several lemmas.

Given a vector $\vec{K} = (k_0, k_1, \dots, k_n) \in \mathbb{Z}_{\geq 0}^{n+1}$, we can obtain a prolongation of \mathbb{P} :

$$\mathbb{P}[\vec{K}] = \bigcup_{i=0}^n \mathbf{N}(\mathbb{P}_i)^{[k_i]}. \quad (8)$$

Let $t_j = \max\{s_{0j} + k_0, s_{1j} + k_1, \dots, s_{nj} + k_n\}$. Then $\mathbb{P}^{[\vec{K}]}$ is contained in $\mathbb{Q}[\mathbf{u}^{[\vec{K}]}, \mathbb{Y}^{[\vec{K}]}]$, where $\mathbf{u}^{[\vec{K}]} = \cup_{i=0}^n \mathbf{u}_i^{[k_i]}$ and $\mathbb{Y}^{[\vec{K}]} = \cup_{j=1}^n y_j^{[t_j]}$.

Denote $\nu(\mathbb{P}^{[\vec{K}]})$ to be the number of \mathbb{Y} and their transforms appearing effectively in $\mathbb{P}^{[\vec{K}]}$. In order to derive a difference relation among \mathbf{u}_i ($i = 0, \dots, n$) from $\mathbb{P}^{[\vec{K}]}$, a sufficient condition is

$$|\mathbb{P}^{[\vec{K}]}| \geq \nu(\mathbb{P}^{[\vec{K}]}) + 1. \quad (9)$$

Note that $\nu(\mathbb{P}^{[\vec{K}]}) \leq |\mathbb{Y}^{[\vec{K}]}| = \sum_{j=1}^n (t_j + 1)$. Thus, if $|\mathbb{P}^{[\vec{K}]}| \geq |\mathbb{Y}^{[\vec{K}]}| + 1$, or equivalently,

$$k_0 + k_1 + \dots + k_n \geq \sum_{j=1}^n \max(s_{0j} + k_0, s_{1j} + k_1, \dots, s_{nj} + k_n) \quad (10)$$

is satisfied, then so is the inequality (9).

Lemma 4.9 *Let \mathbb{P} be a Laurent transformally essential system and $\vec{K} = (k_0, k_1, \dots, k_n) \in \mathbb{Z}_{\geq 0}^{n+1}$ a vector satisfying (10). Then $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq k_i$ for each $i = 0, \dots, n$.*

Proof: Denote $\mathfrak{m}^{[\vec{K}]}$ to be the set of all monomials in variables $\mathbb{Y}^{[\vec{K}]}$. Let $\mathcal{I} = (\mathbb{P}^{[\vec{K}]}) : \mathfrak{m}^{[\vec{K}]}$ be an ideal in the polynomial ring $\mathbb{Q}[\mathbb{Y}^{[\vec{K}]}, \mathbf{u}^{[\vec{K}]}]$. Denote $U = \mathbf{u}^{[\vec{K}]} \setminus \cup_{i=0}^n u_{i0}^{[k_i]}$. Let $\zeta_{il} = -(\sum_{k=1}^{l_i} u_{ik} M_{ik} / M_{i0})^{(l)}$ for $i = 0, 1, \dots, n; l = 0, 1, \dots, k_i$. Denote $\zeta = (U, \zeta_{0k_0}, \dots, \zeta_{00}, \dots, \zeta_{nk_n}, \dots, \zeta_{n0})$. It is easy to show that $(\mathbb{Y}^{[\vec{K}]}, \zeta)$ is a generic point of \mathcal{I} . Let $\mathcal{I}_1 = \mathcal{I} \cap \mathbb{Q}[\mathbf{u}^{[\vec{K}]}]$. Then \mathcal{I}_1 is a prime ideal with a generic point ζ . Since $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\mathbb{Y}^{[\vec{K}]}, U)$, $\text{Codim}(\mathcal{I}_1) = |U| + \sum_{i=0}^n (k_i + 1) - \text{tr.deg } \mathbb{Q}(\zeta) / \mathbb{Q} \geq |U| + |\mathbb{P}^{[\vec{K}]}| - \text{tr.deg } \mathbb{Q}(\mathbb{Y}^{[\vec{K}]}, U) / \mathbb{Q} = |\mathbb{P}^{[\vec{K}]}| - |\mathbb{Y}^{[\vec{K}]}| \geq 1$. Thus, $\mathcal{I}_1 \neq \{0\}$. Suppose f is a nonzero polynomial in \mathcal{I}_1 . Clearly, $\text{ord}(f, \mathbf{u}_i) \leq k_i$ and $f \in [\mathbb{P}] : \mathfrak{m} \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$. By Lemma 3.9 and Lemma 4.8, $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq \text{ord}(f, \mathbf{u}_i) \leq k_i$. \square

Lemma 4.10 [23, Lemma 5.6] *Let \mathbb{P} be a system with $J_i \geq 0$ for each $i = 0, \dots, n$. Then $k_i = J_i$ ($i = 0, \dots, n$) satisfy (10) in the equality case.*

Corollary 4.11 *Let \mathbb{P} be a Laurent transformally essential system and $J_i \geq 0$ for each $i = 0, \dots, n$. Then $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq J_i$ ($i = 0, \dots, n$).*

Proof: It is a direct consequence of Lemma 4.9 and Lemma 4.10. \square

The above corollary shows that when all the Jacobi numbers are not less than 0, then Jacobi numbers are order bounds for the sparse difference resultant. In the following, we deal with the remaining case when some $J_i = -\infty$. To this end, two more lemmas are needed.

Lemma 4.12 [6, 20] *Let A be an $m \times n$ matrix whose entries are 0's and 1's. Let $\text{Jac}(A) = J < \min\{m, n\}$. Then A contains an $a \times b$ zero sub-matrix with $a + b = m + n - J$.*

Lemma 4.13 *Let \mathbb{P} be a Laurent transformally essential system with the following $(n+1) \times n$ order matrix*

$$A = \begin{pmatrix} A_{11} & (-\infty)_{r \times t} \\ A_{21} & A_{22} \end{pmatrix},$$

where $r + t \geq n + 1$. Then $r + t = n + 1$ and $\text{Jac}(A_{22}) \geq 0$. Moreover, when regarded as difference polynomials in y_1, \dots, y_{r-1} , $\{\mathbb{P}_0, \dots, \mathbb{P}_{r-1}\}$ is a Laurent transformally essential system.

Proof: The proof is similar to [23, Lemma 5.9]. □

Theorem 4.14 *Let \mathbb{P} be a Laurent transformally essential system and \mathbf{R} the sparse difference resultant of \mathbb{P} . Then*

$$\text{ord}(\mathbf{R}, \mathbf{u}_i) = \begin{cases} -\infty & \text{if } J_i = -\infty, \\ h_i \leq J_i & \text{if } J_i \geq 0. \end{cases}$$

Proof: Corollary 4.11 proves the case when $J_i \geq 0$ for each i . Now suppose there exists at least one i such that $J_i = -\infty$. Without loss of generality, we assume $J_n = -\infty$ and let $A_n = (s_{ij})_{0 \leq i \leq n-1; 1 \leq j \leq n}$ be the order matrix of $\mathbb{P}_{\hat{n}}$. By Lemma 4.12, we can assume that A_n is of the following form

$$A_n = \begin{pmatrix} A_{11} & (-\infty)_{r \times t} \\ \bar{A}_{21} & \bar{A}_{22} \end{pmatrix},$$

where $r + t \geq n + 1$. Then the order matrix of \mathbb{P} is equal to

$$A = \begin{pmatrix} A_{11} & (-\infty)_{r \times t} \\ A_{21} & A_{22} \end{pmatrix}.$$

Since \mathbb{P} is Laurent transformally essential, by Lemma 4.13, $r + t = n + 1$ and $\text{Jac}(A_{22}) \geq 0$. Moreover, considered as difference polynomials in y_1, \dots, y_{r-1} , $\tilde{\mathbb{P}} = \{p_0, \dots, p_{r-1}\}$ is Laurent transformally essential and A_{11} is its order matrix. Let $\tilde{J}_i = \text{Jac}((A_{11})_i)$. By applying the above procedure when necessary, we can suppose that $\tilde{J}_i \geq 0$ for each $i = 0, \dots, r - 1$. Since $[\mathbb{P}] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\} = [\tilde{\mathbb{P}}] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_{r-1}\}$, \mathbf{R} is also the sparse difference resultant of the system $\tilde{\mathbb{P}}$ and $\mathbf{u}_r, \dots, \mathbf{u}_n$ will not occur in \mathbf{R} . By Corollary 4.11, $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq \tilde{J}_i$. Since $J_i = \text{Jac}(A_{22}) + \tilde{J}_i \geq \tilde{J}_i$ for $0 \leq i \leq r - 1$, $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq J_i$ for $0 \leq i \leq r - 1$ and $\text{ord}(\mathbf{R}, \mathbf{u}_i) = -\infty$ for $i = r, \dots, n$. □

Example 4.15 *Let $n = 2$ and \mathbb{P}_i has the form*

$$\mathbb{P}_0 = u_{00} + u_{01}y_1y_1^{(1)}, \mathbb{P}_1 = u_{10} + u_{11}y_1, \mathbb{P}_2 = u_{10} + u_{11}y_2^{(1)}.$$

In this example, the order matrix of \mathbb{P} is $A = \begin{pmatrix} 1 & -\infty \\ 0 & -\infty \\ -\infty & 1 \end{pmatrix}$. Thus $J_0 = 1, J_1 = 2, J_2 = -\infty$. And $\text{ord}(\mathbf{R}, \mathbf{u}_0) = 0 < J_0, \text{ord}(\mathbf{R}, \mathbf{u}_1) = 1 < J_1, \text{ord}(\mathbf{R}, \mathbf{u}_2) = -\infty$.

Corollary 4.16 *Let \mathbb{P} be supper-essential. Then $J_i \geq 0$ for $i = 0, \dots, n$ and $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq J_i$.*

Proof: From the proof of Theorem 4.14, if $J_i = -\infty$ for some i , then \mathbb{P} contains a proper transformally essential subsystem, which contradicts to Theorem 3.24. Therefore, $J_i \geq 0$ for $i = 0, \dots, n$. \square

We conclude this section by giving two improved order bounds based on the Jacobi bound given in Theorem 4.14.

For each $j \in \{1, \dots, n\}$, let $\underline{o}_j = \min\{k \in \mathbb{N}_0 \mid \exists i \text{ s.t. } \deg(N(\mathbb{P}_i), y_j^{(k)}) > 0\}$. In other words, \underline{o}_j is the smallest number such that $y_j^{(\underline{o}_j)}$ occurs in $\{N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)\}$. Let $B = (s_{ij} - \underline{o}_j)$ be an $(n+1) \times n$ matrix. We call $\bar{J}_i = \text{Jac}(B_i)$ the *modified Jacobi number* of the system \mathbb{P}_i . Denote $\underline{\gamma} = \sum_{j=1}^n \underline{o}_j$. Clearly, $\bar{J}_i = J_i - \underline{\gamma}$. Then we have the following result.

Theorem 4.17 *Let \mathbb{P} be a Laurent transformally essential system and \mathbf{R} the sparse difference resultant of \mathbb{P} . Then*

$$\text{ord}(\mathbf{R}, \mathbf{u}_i) = \begin{cases} -\infty & \text{if } J_i = -\infty, \\ h_i \leq J_i - \underline{\gamma} & \text{if } J_i \geq 0. \end{cases}$$

Proof: The proof is similar to [23, Theorem 5.13]. \square

Now, we assume that \mathbb{P} is a Laurent transformally essential system which is not super-essential. Let \mathbf{R} be the sparse difference resultant of \mathbb{P} . We will give a better order bound for \mathbf{R} . By Theorem 3.24, \mathbb{P} contains a unique super-essential sub-system $\mathbb{P}_{\mathbb{T}}$. Without loss of generality, suppose $\mathbb{T} = \{0, \dots, r\}$ with $r < n$. Let $A_{\mathbb{T}}$ be the order matrix of $\mathbb{P}_{\mathbb{T}}$ and for $i = 0, \dots, r$, let $(A_{\mathbb{T}})_i$ be the matrix obtained from $A_{\mathbb{T}}$ by deleting the $(i+1)$ -th row. Note that $(A_{\mathbb{T}})_i$ is an $r \times n$ matrix. Then we have the following result.

Theorem 4.18 *With the above notations, we have*

$$\text{ord}(\mathbf{R}, \mathbf{u}_i) = \begin{cases} h_i \leq \text{Jac}((A_{\mathbb{T}})_i) & i = 0, \dots, r, \\ -\infty & i = r+1, \dots, n. \end{cases}$$

Proof: Similarly to the proof of [23, Theorem 5.16], it can be proved. \square

Example 4.19 *Continue from Example 4.15. In this example, $\mathbb{T} = \{0, 1\}$. Then $A_{\mathbb{T}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Thus $\text{Jac}((A_{\mathbb{T}})_{\emptyset}) = 0$, $\text{Jac}((A_{\mathbb{T}})_1) = 1$. And $\text{ord}(\mathbf{R}, \mathbf{u}_0) = 0 = \text{Jac}((A_{\mathbb{T}})_{\emptyset})$, $\text{ord}(\mathbf{R}, \mathbf{u}_1) = 1 = \text{Jac}((A_{\mathbb{T}})_1)$, $\text{ord}(\mathbf{R}, \mathbf{u}_2) = -\infty$.*

5 A single exponential algorithm to compute the sparse difference resultant

In this section, we give an algorithm to compute the sparse difference resultant for a Laurent transformally essential system with single exponential complexity. The idea is to estimate the degree bounds for the resultant and then to use linear algebra to find the coefficients of the resultant.

5.1 Degree bound for sparse difference resultant

In this section, we give an upper bound for the degree of the sparse difference resultant, which will be crucial to our algorithm to compute the sparse resultant. Before proposing the main theorem, we first give some algebraic results which will be needed in the proof.

Lemma 5.1 [23, Theorem 6.2] *Let \mathcal{I} be a prime ideal in $K[x_1, \dots, x_n]$ and $\mathcal{I}_k = \mathcal{I} \cap K[x_1, \dots, x_k]$ for any $1 \leq k \leq n$. Then $\deg(\mathcal{I}_k) \leq \deg(\mathcal{I})$.*

Lemma 5.2 [28, Corollary 2.28] *Let $V_1, \dots, V_r \subset \mathbf{P}^n$ ($r \geq 2$) be pure dimensional projective varieties in \mathbf{P}^n . Then*

$$\prod_{i=1}^r \deg(V_i) \geq \sum_C \deg(C)$$

where C runs through all irreducible components of $V_1 \cap \dots \cap V_r$.

Now we are ready to give the main theorem of this section.

Theorem 5.3 *Let $\mathbb{P}_0, \dots, \mathbb{P}_n$ be a Laurent transformally essential system of form (1) with $\text{ord}(\mathbb{N}(\mathbb{P}_i)) = s_i$ and $\deg(\mathbb{N}(\mathbb{P}_i), \mathbb{Y}) = m_i$. Suppose $\mathbb{N}(\mathbb{P}_i) = \sum_{k=0}^{l_i} u_{ik} N_{ik}$ and J_i is the Jacobi number of $\{\mathbb{N}(\mathbb{P}_0), \dots, \mathbb{N}(\mathbb{P}_n)\} \setminus \{\mathbb{N}(\mathbb{P}_i)\}$. Denote $m = \max_i \{m_i\}$. Let $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ be the sparse difference resultant of \mathbb{P}_i ($i = 0, \dots, n$). Suppose $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i$ for each i . Then the following assertions hold:*

- 1) $\deg(\mathbf{R}) \leq \prod_{i=0}^n (m_i + 1)^{h_i+1} \leq (m + 1)^{\sum_{i=0}^n (J_i+1)}$, where $m = \max_i \{m_i\}$.
- 2) \mathbf{R} has a representation

$$\prod_{i=0}^n \prod_{k=0}^n (N_{i0}^{(k)})^{\deg(\mathbf{R})} \cdot \mathbf{R} = \sum_{i=0}^n \sum_{k=0}^{h_i} G_{ik} \mathbb{N}(\mathbb{P}_i)^{(k)} \quad (11)$$

where $G_{ik} \in \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}, \mathbb{Y}^{[h]}]$ and $h = \max\{h_i + e_i\}$ such that $\deg(G_{ik} \mathbb{N}(\mathbb{P}_i)^{(k)}) \leq [m + 1 + \sum_{i=0}^n (h_i + 1) \deg(N_{i0})] \deg(\mathbf{R})$.

Proof: In \mathbf{R} , let u_{i0} be replaced by $(\mathbb{N}(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik} N_{ik}) / N_{i0}$ for each $i = 0, \dots, n$ and let \mathbf{R} be expanded as a difference polynomial in $\mathbb{N}(\mathbb{P}_i)$ and their transforms. Then there exist $a_{ik} \in \mathbb{N}$ and polynomials G_{ik} such that $\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{a_{ik}} \mathbf{R} = \sum_{i=0}^n \sum_{k=0}^{h_i} G_{ik} \mathbb{N}(\mathbb{P}_i)^{(k)} + T$ with $T \in \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\}$ free from u_{i0} . Since $T \in \mathcal{I} = [\mathbb{N}(\mathbb{P}_0), \dots, \mathbb{N}(\mathbb{P}_n)] : \mathfrak{m}$, T vanishes identically, for $\mathcal{I} \cap \mathbb{Q}\{\mathbf{u}, \mathbb{Y}\} = \{0\}$ by Theorem 3.6. Thus,

$$\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{a_{ik}} \mathbf{R} = \sum_{i=0}^n \sum_{k=0}^{h_i} G_{ik} \mathbb{N}(\mathbb{P}_i)^{(k)}.$$

1) Let $\mathcal{J} = (\mathbb{N}(\mathbb{P}_0)^{[h_0]}, \dots, \mathbb{N}(\mathbb{P}_n)^{[h_n]}) : \mathfrak{m}^{[h]}$ be an algebraic ideal in $\mathcal{R} = \mathbb{Q}[\mathbb{Y}^{[h]}, \mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}]$ where $h = \max_i \{h_i + s_i\}$ and $\mathfrak{m}^{[h]}$ is the set of all monomials in $\mathbb{Y}^{[h]}$. Then $\mathbf{R} \in \mathcal{J}$ by the above equality. Let $\eta = (\eta_1, \dots, \eta_n)$ be a generic point of $[0]$ over $\mathbb{Q}(\mathbf{u})$

and denote $\zeta_i = -\sum_{k=1}^{l_i} u_{ik} \frac{N_{ik}(\eta)}{N_{i0}(\eta)}$ ($i = 0, \dots, n$). It is easy to show that \mathcal{J} is a prime ideal in \mathcal{R} with a generic point $(\eta^{[h]}; \tilde{\mathbf{u}}, \zeta_0^{[h_0]}, \dots, \zeta_n^{[h_n]})$ and $\mathcal{J} \cap \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}] = (\mathbf{R})$, where $\tilde{\mathbf{u}} = \cup_i \mathbf{u}_i^{[h_i]} \setminus \{u_{i0}^{[h_i]}\}$. Let H_{ik} be the homogeneous polynomial corresponding to $N(\mathbb{P}_i)^{(k)}$ with x_0 the variable of homogeneity. Then $\mathcal{J}^0 = ((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i}) : \tilde{\mathbf{m}}$ is a prime ideal in $\mathbb{Q}[x_0, \mathbb{Y}^{[h]}, \mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}]$ where $\tilde{\mathbf{m}}$ is the whole set of monomials in $\mathbb{Y}^{[h]}$ and x_0 . And $\deg(\mathcal{J}^0) = \deg(\mathcal{J})$.

Since $\mathbb{V}((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i}) = \mathbb{V}(\mathcal{J}^0) \cup \mathbb{V}(H_{ik}, x_0) \cup \cup_{j,l} \mathbb{V}(H_{ik}, y_j^{(l)})$, $\mathbb{V}(\mathcal{J}^0)$ is an irreducible component of $\mathbb{V}((H_{ik})_{1 \leq i \leq n; 0 \leq k \leq h_i})$. By Lemma 5.2, $\deg(\mathcal{J}^0) \leq \prod_{i=0}^n \prod_{k=0}^{h_i} (m_i + 1) = \prod_{i=0}^n (m_i + 1)^{h_i+1}$. Thus, $\deg(\mathcal{J}) \leq \prod_{i=0}^n (m_i + 1)^{h_i+1}$. Since $\mathcal{J} \cap \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}] = (\mathbf{R})$, by Lemma 5.1, $\deg(\mathbf{R}) \leq \deg(\mathcal{J}) \leq \prod_{i=0}^n (m_i + 1)^{h_i+1} \leq (m+1)^{\sum_{i=0}^n (J_i+1)}$ follows. The last inequality holds because $h_i \leq J_i$ by Theorem 4.17.

2) To obtain the degree bounds for the above representation of \mathbf{R} , that is, to estimate $\deg(G_{ik}N(\mathbb{P}_i)^{(k)})$ and a_{ik} , we take each monomial M in \mathbf{R} and substitute u_{i0} by $(N(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik} N_{ik})/N_{i0}$ into M and then expand it. To be more precise, we take one monomial $M(\mathbf{u}; u_{00}, \dots, u_{n0}) = \mathbf{u}^\gamma \prod_{i=0}^n \prod_{k=0}^{h_i} (u_{i0}^{(k)})^{d_{ik}}$ with $|\gamma| + \sum_{i=0}^n \sum_{k=0}^{h_i} d_{ik} = \deg(\mathbf{R})$ for an example, where \mathbf{u}^γ represents a difference monomial in \mathbf{u} and their transforms with exponent vector γ . Then

$$M(\mathbf{u}; u_{00}, \dots, u_{n0}) = \mathbf{u}^\gamma \prod_{i=0}^n \prod_{k=0}^{h_i} \left((N(\mathbb{P}_i) - \sum_{k=1}^{l_i} u_{ik} N_{ik})^{(k)} \right)^{d_{ik}} / \prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{d_{ik}}.$$

When expanded, every term of $\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{d_{ik}} M$ is of degree bounded by $|\gamma| + \sum_{i=0}^n \sum_{k=0}^{h_i} (m_i + 1) d_{ik} \leq (m+1) \deg(\mathbf{R})$ in $\mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}$ and $\mathbb{Y}^{[h]}$. Suppose $\mathbf{R} = \sum_M a_M M$ and $a_{ik} \geq \max_M \{d_{ik}\}$. Then

$$\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^{a_{ik}} \mathbf{R} = \sum_{i=0}^n \sum_{k=0}^{h_i} G_{ik} N(\mathbb{P}_i)^{(k)}$$

with $\deg(G_{ik}N(\mathbb{P}_i)^{(k)}) \leq (m+1) \deg(\mathbf{R}) + \sum_{i=0}^n \sum_{k=0}^{h_i} \deg(N_{i0}) a_{ik}$. Clearly, we can take $a_{ik} = \deg(\mathbf{R})$ and then $\deg(G_{ik}N(\mathbb{P}_i)^{(k)}) \leq (m+1 + \sum_{i=0}^n (h_i + 1) \deg(N_{i0})) \deg(\mathbf{R})$. Thus, (11) follows. \square

For a transformally essential difference polynomial system with degree 0 terms, the second part of Theorem 5.3 can be improved as follows.

Corollary 5.4 *Let $\mathbb{P}_i = u_{i0} + \sum_{k=1}^{l_i} u_{ik} N_{ik}$ ($i = 0, \dots, n$) be a transformally essential difference polynomial system with $m = \max_i \{\deg(\mathbb{P}_i, \mathbb{Y})\}$ and J_i the Jacobi number of $\{\mathbb{P}_0, \dots, \mathbb{P}_n\} \setminus \{\mathbb{P}_i\}$. Let $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ be the sparse difference resultant of \mathbb{P}_i ($i = 0, \dots, n$). Suppose $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i$ for each i and $h = \max\{h_i + s_i\}$. Then \mathbf{R} has a representation*

$$\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n) = \sum_{i=0}^n \sum_{j=0}^{h_i} G_{ij} \mathbb{P}_i^{(j)}$$

where $G_{ij} \in \mathbb{Q}[\mathbf{u}_0^{[h_0]}, \dots, \mathbf{u}_n^{[h_n]}, \mathbb{Y}^{[h]}]$ such that $\deg(G_{ij} \mathbb{P}_i^{(j)}) \leq (m+1) \deg(\mathbf{R}) \leq (m+1)^{\sum_{i=0}^n (J_i+1)+1}$.

Proof: It is direct consequence of Theorem 5.3 by setting $N_{i0} = 1$. \square

The following result gives an effective difference Nullstellensatz under certain conditions.

Corollary 5.5 *Let $f_0, \dots, f_n \in \mathcal{F}\{y_1, \dots, y_n\}$ have no common solutions with $\deg(f_i) \leq m$. Let $\text{Jac}(\{f_0, \dots, f_n\} \setminus \{f_i\}) = J_i$. If the sparse difference resultant of f_0, \dots, f_n is nonzero, then there exist $H_{ij} \in \mathcal{F}\{y_1, \dots, y_n\}$ s.t. $\sum_{i=0}^n \sum_{j=0}^{J_i} H_{ij} f_i^{(j)} = 1$ and $\deg(H_{ij} f_i^{(j)}) \leq (m+1) \sum_{i=0}^n (J_i+1)+1$.*

Proof: The hypothesis implies that $\mathbb{P}(f_i)$ form a transformally essential system. Clearly, $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ has the property stated in Corollary 5.4, where \mathbf{u}_i are coefficients of $\mathbb{P}(f_i)$. The result follows directly from Corollary 5.4 by specializing \mathbf{u}_i to the coefficients of f_i . \square

5.2 A single exponential algorithm to compute sparse difference resultant

If a polynomial R is the linear combination of some known polynomials $F_i (i = 1, \dots, s)$, that is $R = \sum_{i=1}^s H_i F_i$, and we know the upper bounds of the degrees of R and $H_i F_i$, then a general idea to estimate the computational complexity of R is to use linear algebra to find the coefficients of R .

For sparse difference resultant, we already have given its degree bound and the degrees of the expressions in the linear combination in Theorem 5.3.

Now, we give the algorithm **SDResultant** to compute sparse difference resultants based on the linear algebra techniques. The algorithm works adaptively by searching for \mathbf{R} with an order vector $(h_0, \dots, h_n) \in \mathbb{N}_0^{n+1}$ with $h_i \leq J_i$ by Theorem 5.3. Denote $o = \sum_{i=0}^n h_i$. We start with $o = 0$. And for this o , choose one vector (h_0, \dots, h_n) at a time. For this (h_0, \dots, h_n) , we search for \mathbf{R} from degree $d = 1$. If we cannot find an \mathbf{R} with such a degree, then we repeat the procedure with degree $d+1$ until $d > \prod_{i=0}^n (m_i+1)^{h_i+1}$. In that case, we choose another (h_0, \dots, h_n) with $\sum_{i=0}^n h_i = o$. But if for all (h_0, \dots, h_n) with $h_i \leq J_i$ and $\sum_{i=0}^n h_i = o$, \mathbf{R} cannot be found, then we repeat the procedure with $o+1$. In this way, we will find an \mathbf{R} with the smallest order satisfying equation (11), which is the sparse resultant.

Theorem 5.6 *Let $\mathbb{P}_0, \dots, \mathbb{P}_n$ be a Laurent transformally essential system of form (1). Denote $\mathbb{P} = \{N(\mathbb{P}_0), \dots, N(\mathbb{P}_n)\}$, $J_i = \text{Jac}(\mathbb{P}_i)$, $J = \max_i J_i$ and $m = \max_{i=0}^n \deg(\mathbb{P}_i, \mathbb{Y})$. Algorithm **SDResultant** computes sparse difference resultant \mathbf{R} of $\mathbb{P}_0, \dots, \mathbb{P}_n$ with the following complexities:*

1) *In terms of the degree bound D of \mathbf{R} , the algorithm needs at most $O(D^{O(lJ)}(nJ)^{O(lJ)})$ \mathbb{Q} -arithmetic operations, where $l = \sum_{i=0}^n (l_i + 1)$ is the size of all \mathbb{P}_i .*

2) *The algorithm needs at most $O(m^{O(nlJ^2)}(nJ)^{O(lJ)})$ \mathbb{Q} -arithmetic operations.*

Proof: The algorithm finds a difference polynomial P in $\mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ satisfying equation (11), which has the smallest order and the smallest degree in those with the same order. Existence for such a difference polynomial is guaranteed by Theorem 5.3. By the definition of sparse difference resultant, P must be \mathbf{R} .

We will estimate the complexity of the algorithm below. Denote D to be the degree bound of \mathbf{R} . By Theorem 5.3, $D \leq (m+1) \sum_{i=0}^n (J_i+1)$. In each loop of Step 3, the complexity

Algorithm 1 — **SDResultant**($\mathbb{P}_0, \dots, \mathbb{P}_n$)

Input: A generic Laurent transformally essential system $\mathbb{P}_0, \dots, \mathbb{P}_n$.

Output: The sparse difference resultant $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ of $\mathbb{P}_0, \dots, \mathbb{P}_n$.

1. For $i = 0, \dots, n$, set $N(P_i) = \sum_{k=0}^{l_i} u_{ik} N_{ik}$ with $\deg(N_{i0}) \leq \deg(N_{ik})$.
Set $m_i = \deg(N(\mathbb{P}_i))$, $m_{i0} = \deg(N_{i0})$, $\mathbf{u}_i = \text{coeff}(\mathbb{P}_i)$ and $|\mathbf{u}_i| = l_i + 1$.
Set $s_{ij} = \text{ord}(N(\mathbb{P}_i), y_j)$, $A = (s_{ij})$ and compute $J_i = \text{Jac}(A_i)$.
2. Set $\mathbf{R} = 0$, $o = 0$, $m = \max_i \{m_i\}$.
3. While $\mathbf{R} = 0$ do
 - 3.1. For each $(h_0, \dots, h_n) \in \mathbb{N}_0^{n+1}$ with $\sum_{i=0}^n h_i = o$ and $h_i \leq J_i$ do
 - 3.1.1. $U = \cup_{i=0}^n \mathbf{u}_i^{[h_i]}$, $h = \max_i \{h_i + e_i\}$, $d = 1$.
 - 3.1.2. While $\mathbf{R} = 0$ and $d \leq \prod_{i=0}^n (m_i + 1)^{h_i+1}$ do
 - 3.1.2.1. Set \mathbf{R}_0 to be a homogeneous GPol of degree d in U .
 - 3.1.2.2. Set $\mathbf{c}_0 = \text{coeff}(\mathbf{R}_0, U)$.
 - 3.1.2.3. Set $H_{ij}(i = 0, \dots, n; j = 0, \dots, h_i)$ to be GPols of degree $[m + 1 + \sum_{i=0}^n (h_i + 1)m_{i0}]d - m_i - 1$ in $\mathbb{Y}^{[h]}, U$.
 - 3.1.2.4. Set $\mathbf{c}_{ij} = \text{coeff}(H_{ij}, \mathbb{Y}^{[h]} \cup U)$.
 - 3.1.2.5. Set \mathcal{P} to be the set of coefficients of $\prod_{i=0}^n \prod_{k=0}^{h_i} (N_{i0}^{(k)})^d \mathbf{R}_0 - \sum_{i=0}^n \sum_{j=0}^{h_i} H_{ij} (N(\mathbb{P}_i))^{(j)}$ as a polynomial in $\mathbb{Y}^{[h]}, U$.
 - 3.1.2.6. Solve the linear equation $\mathcal{P} = 0$ in variables \mathbf{c}_0 and \mathbf{c}_{ij} .
 - 3.1.2.7. If \mathbf{c}_0 has a nonzero solution, then substitute it into \mathbf{R}_0 to get \mathbf{R} and go to Step 4, else $\mathbf{R} = 0$.
 - 3.1.2.8. $d := d + 1$.
 - 3.2. $o := o + 1$.
 4. Return \mathbf{R} .

/*/ GPol stands for generic algebraic polynomial.

/*/ $\text{coeff}(P, V)$ returns the set of coefficients of P as an ordinary polynomial in variables V .

of the algorithm is clearly dominated by Step 3.1.2, where we need to solve a system of linear equations $\mathcal{P} = 0$ over \mathbb{Q} in \mathbf{c}_0 and \mathbf{c}_{ij} . It is easy to show that $|\mathbf{c}_0| = \binom{d+L-1}{L-1}$ and $|\mathbf{c}_{ij}| = \binom{d_1 - m_i - 1 + L + n(h+1)}{L+n(h+1)}$, where $L = \sum_{i=0}^n (h_i + 1)(l_i + 1)$ and $d_1 = [m + 1 + \sum_{i=0}^n (h_i + 1)m_{i0}]d$. Then $\mathcal{P} = 0$ is a linear equation system with $N = \binom{d+L-1}{L-1} + \sum_{i=0}^n (h_i + 1) \binom{d_1 - m_i - 1 + L + n(h+1)}{L+n(h+1)}$ variables and $M = \binom{d_1 + L + n(h+1)}{L+n(h+1)}$ equations. To solve it, we need at most $(\max\{M, N\})^\omega$ arithmetic operations over \mathbb{Q} , where ω is the matrix multiplication exponent and the currently best known ω is 2.376.

The iteration in Step 3.1.2 may go through 1 to $\prod_{i=0}^n (m_i + 1)^{h_i+1} \leq (m + 1)^{\sum_{i=0}^n (J_i+1)}$, and the iteration in Step 3.1 at most will repeat $\prod_{i=0}^n (J_i + 1) \leq (n + 1)(J + 1)$ times, where $J = \max_i J_i$. And by Theorem 5.3, Step 3 may loop from $o = 0$ to $\sum_{i=0}^n (J_i + 1)$. The whole

algorithm needs at most

$$\begin{aligned} & \sum_{o=0}^{\sum_{i=0}^n (J_i+1)} \sum_{\substack{h_i \leq J_i \\ \sum_i h_i = o}} \sum_{d=1}^{\prod_{i=0}^n (m_i+1)^{h_i+1}} (\max\{M, N\})^{2.376} \\ & \leq O(D^{O(lJ)}(nJ)^{O(lJ)}) \leq O(m^{O(nlJ^2)}(nJ)^{O(lJ)}) \end{aligned}$$

arithmetic operations over \mathbb{Q} . In the above inequalities, we assume that $(m+1)^{\sum_{i=0}^n (J_i+1)+1} \geq l(n+1)J$ and $l \geq (n+1)^2$, where $l = \sum_{i=0}^n (l_i+1)$. Our complexity assumes an $O(1)$ -complexity cost for all field operations over \mathbb{Q} . Thus, the complexity follows. \square

Remark 5.7 *As we indicated at the end of Section 3.3, if we first compute the super-essential set \mathbb{T} , then the algorithm can be improved by only considering the Laurent difference polynomials \mathbb{P}_i ($i \in \mathbb{T}$) in the linear combination of the sparse resultant.*

Remark 5.8 *Algorithm **SDResultant** can be improved by using a better search strategy. If d is not big enough, instead of checking $d+1$, we can check $2d$. Repeating this procedure, we may find a k such that $2^k \leq \deg(\mathbf{R}) \leq 2^{k+1}$. We then bisecting the interval $[2^k, 2^{k+1}]$ again to find the proper degree for \mathbf{R} . This will lead to a better complexity, which is still single exponential.*

For difference polynomials with non-vanishing degree terms, a better degree bound is given in Corollary 5.4. Based on this bound, we can simplify the Algorithm **SDResultant** to compute the sparse difference resultant by removing the computation for $N(P_i)$ and N_{i0} in the first step where N_{i0} is exactly equal to 1.

Theorem 5.9 *Algorithm **SDResultant** computes sparse difference resultants for a transformally essential system of the form $\mathbb{P}_i = u_{i0} + \sum_{k=1}^{l_i} u_{ik}N_{ik}$ with at most $O(n^{3.376}J^{O(n)}m^{O(nlJ^2)})$ \mathbb{Q} -arithmetic operations.*

Proof: Follow the proof process of Theorem 5.6, it can be shown that the complexity is $O(n^{3.376}J^{O(n)}m^{O(nlJ^2)})$. \square

6 Difference resultant

In this section, we introduce the notion of difference resultant and prove its basic properties.

Definition 6.1 *Let $\mathbf{m}_{s,r}$ be the set of all difference monomials in \mathbb{Y} of order $\leq s$ and degree $\leq r$. Let $\mathbf{u} = \{u_M\}_{M \in \mathbf{m}_{s,r}}$ be a set of difference indeterminates over \mathbb{Q} . Then,*

$$\mathbb{P} = \sum_{M \in \mathbf{m}_{s,r}} u_M M$$

is called a generic difference polynomial of order s and degree r .

Throughout this section, a generic difference polynomial is assumed to be of degree greater than zero. Let

$$\mathbb{P}_i = u_{i0} + \sum_{\substack{\alpha \in \mathbb{Z}_{\geq 0}^{n(s_i+1)} \\ 1 \leq |\alpha| \leq m_i}} u_{i\alpha} (\mathbb{Y}^{[s_i]})^\alpha \quad (i = 0, 1, \dots, n) \quad (12)$$

be generic Laurent difference polynomials of order s_i , degree m_i , and coefficients \mathbf{u}_i respectively. Since $\{1, y_1, \dots, y_n\}$ is contained in the support of each \mathbb{P}_i , clearly, they form a super-essential system and the sparse difference resultant $\text{Res}_{\mathbb{P}_0, \dots, \mathbb{P}_n}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ exists. We define $\text{Res}_{\mathbb{P}_0, \dots, \mathbb{P}_n}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ to be the *difference resultant* of $\mathbb{P}_0, \dots, \mathbb{P}_n$. That is,

Definition 6.2 *Let \mathbb{P}_i ($i = 0, 1, \dots, n$) be a generic difference polynomial system of the form (12). Then the difference resultant $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ of $\mathbb{P}_0, \dots, \mathbb{P}_n$ is defined as the irreducible difference polynomial contained in $[\mathbb{P}_0, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$ of minimal order in each \mathbf{u}_i , which is unique up to a factor in \mathbb{Q} .*

Difference resultants hold all the properties we have proved for sparse difference resultants in previous sections. Apart from these, in the following, we will show difference resultants possess other better properties. Firstly, we will give the precise degree for the difference resultant, which is of BKK-type [1, 7]. Before doing so, we need some results about algebraic sparse resultants.

Let $\mathcal{K}[\mathbb{X}] = \mathcal{K}[x_1, \dots, x_n]$ be the polynomial ring defined over a field \mathcal{K} . For any vector $\alpha = (a_1, \dots, a_n) \in \mathbb{Z}^n$, denote the Laurent monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ by \mathbb{X}^α . Let $\mathcal{B}_0, \dots, \mathcal{B}_n \subset \mathbb{Z}^n$ be subsets which jointly span the affine lattice \mathbb{Z}^n . Suppose $\mathbf{0} = (0, \dots, 0) \in \mathcal{B}_i$ for each i and $|\mathcal{B}_i| = l_i + 1 \geq 2$. Let

$$\mathbb{F}_i(x_1, \dots, x_n) = c_{i0} + \sum_{\alpha \in \mathcal{B}_i \setminus \{\mathbf{0}\}} c_{i,\alpha} \mathbb{X}^\alpha \quad (i = 0, 1, \dots, n) \quad (13)$$

be generic sparse Laurent polynomials defined w.r.t \mathcal{B}_i ($i = 0, 1, \dots, n$). \mathcal{B}_i or $\{\mathbb{X}^\alpha : \alpha \in \mathcal{B}_i\}$ are called the support of \mathbb{F}_i . Denote $\mathbf{c}_i = (c_{i\alpha})_{\alpha \in \mathcal{B}_i}$ and $\mathbf{c} = \cup_i (\mathbf{c}_i \setminus \{c_{i0}\})$. Let \mathcal{Q}_i be the convex hull of \mathcal{B}_i in \mathbb{R}^n , which is the smallest convex set containing \mathcal{B}_i . \mathcal{Q}_i is also called the *Newton polytope* of \mathbb{F}_i , denoted by $\text{NP}(\mathbb{F}_i)$. In [27], Sturmfels gave the definition of algebraic essential set and proved that a necessary and sufficient condition for the existence of sparse resultant is that there exists a unique subset $\{\mathcal{B}_i\}_{i \in I}$ which is essential. Now, we restate the definition of essential sets in our words for the sake of later use.

Definition 6.3 *Follow the notations introduced above.*

- A collection of $\{\mathcal{B}_i\}_{i \in J}$, or $\{\mathbb{F}_i\}_{i \in J}$ of the form (13), is said to be algebraically independent if $\text{tr.deg } \mathbb{Q}(\mathbf{c})(\mathbb{F}_i - c_{i0} : i \in J) / \mathbb{Q}(\mathbf{c}) = |J|$. Otherwise, they are said to be algebraically dependent.
- A collection of $\{\mathcal{B}_i\}_{i \in I}$ is said to be essential if $\{\mathcal{B}_i\}_{i \in I}$ is algebraically dependent and for each proper subset J of I , $\{\mathcal{B}_i\}_{i \in J}$ are algebraically independent.

In the case that $\{\mathcal{B}_0, \dots, \mathcal{B}_n\}$ is essential, the degree of the sparse resultant can be described by mixed volumes.

Theorem 6.4 ([27]) *Suppose that $\{\mathcal{B}_0, \dots, \mathcal{B}_n\}$ is essential. For each $i \in \{0, 1, \dots, n\}$, the degree of the sparse resultant in \mathbf{c}_i is a positive integer, equal to the mixed volume*

$$\mathcal{M}(\mathcal{Q}_0, \dots, \mathcal{Q}_{i-1}, \mathcal{Q}_{i+1}, \dots, \mathcal{Q}_n) = \sum_{J \subset \{0, \dots, i-1, i+1, \dots, n\}} (-1)^{n-|J|} \text{vol}\left(\sum_{j \in J} \mathcal{Q}_j\right)$$

where $\text{vol}(\mathcal{Q})$ means the n -dimensional volume of $\mathcal{Q} \subset \mathbb{R}^n$ and $\mathcal{Q}_1 + \mathcal{Q}_2$ means the Minkowski sum of \mathcal{Q}_1 and \mathcal{Q}_2 .

Now, we give the first main result of this section.

Theorem 6.5 *Let \mathbb{P}_i ($i = 0, \dots, n$) be generic difference polynomials in $\mathbb{Y} = \{y_1, \dots, y_n\}$ with order s_i , degree m_i , and coefficients \mathbf{u}_i respectively. Let $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ be the difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$. Denote $s = \sum_{i=0}^n s_i$. Then $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ is also the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \dots, \mathbb{P}_n^{[s-s_n]}$ as polynomials in $\mathbb{Y}^{[s]}$, and for each $i \in \{0, 1, \dots, n\}$ and $k = 0, \dots, s - s_i$,*

$$\text{ord}(\mathbf{R}, \mathbf{u}_i) = s - s_i \quad (14)$$

$$\deg(\mathbf{R}, \mathbf{u}_i^{(k)}) = \mathcal{M}((\mathcal{Q}_{jl})_{j \neq i, 0 \leq l \leq s-s_j}, \mathcal{Q}_{i0}, \dots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \dots, \mathcal{Q}_{i,s-s_i}) \quad (15)$$

where \mathcal{Q}_{jl} is the Newton polytope of $\mathbb{P}_j^{(l)}$ as a polynomial in $\mathbb{Y}^{[s]}$ and $\mathbf{u}_i^{(k)} = \{u_{i\alpha}^{(k)}, u_{i\alpha} \in \mathbf{u}_i\}$.

Proof: Regard $\mathbb{P}_i^{(k)}$ ($i = 0, \dots, n; k = 0, \dots, s - s_i$) as polynomials in the $n(s+1)$ variables $\mathbb{Y}^{[s]} = \{y_1, \dots, y_n, y_1^{(1)}, \dots, y_n^{(1)}, \dots, y_1^{(s)}, \dots, y_n^{(s)}\}$, and we denote its support by \mathcal{B}_{ik} . Since the coefficients of $\mathbb{P}_i^{(k)}$ can be treated as algebraic indeterminates, $\mathbb{P}_i^{(k)}$ are generic sparse polynomials with supports \mathcal{B}_{ik} respectively. Now we claim that:

C1) $\overline{\mathcal{B}} = \{\mathcal{B}_{ik} : 0 \leq i \leq n; 0 \leq k \leq s - s_i\}$ is an essential set.

C2) $\overline{\mathcal{B}} = \{\mathcal{B}_{ik} : 0 \leq i \leq n; 0 \leq k \leq s - s_i\}$ jointly spans the affine lattice $\mathbb{Z}^{n(s+1)}$.

Note that $|\overline{\mathcal{B}}| = n(s+1) + 1$. To prove C1), it suffices to show that any $n(s+1)$ of distinct $\mathbb{P}_i^{(k)}$ are algebraically independent. Without loss of generality, we prove that for a fixed $l \in \{0, \dots, s - s_0\}$,

$$S_l = \{(\mathbb{P}_i^{(k)})_{1 \leq i \leq n; 0 \leq k \leq s-s_i}, \mathbb{P}_0, \dots, \mathbb{P}_0^{(l-1)}, \mathbb{P}_0^{(l+1)}, \dots, \mathbb{P}_0^{(s-s_0)}\}$$

is an algebraically independent set. Clearly, $\{y_j^{(k)}, \dots, y_j^{(s_i+k)} \mid j = 1, \dots, n\}$ is a subset of the support of $\mathbb{P}_i^{(k)}$. Now we choose a monomial from each $\mathbb{P}_i^{(k)}$ and denote it by $m(\mathbb{P}_i^{(k)})$. Let

$$m(\mathbb{P}_0^{(k)}) = \begin{cases} y_1^{(k)} & 0 \leq k \leq l-1 \\ y_1^{(s_0+k)} & l+1 \leq k \leq s-s_0 \end{cases} \quad \text{and} \quad m(\mathbb{P}_1^{(k)}) = \begin{cases} y_1^{(l+k)} & 0 \leq k \leq s_0 \\ y_2^{(s_1+k)} & s_0+1 \leq k \leq s-s_1 \end{cases}.$$

For each $i \in \{2, \dots, n\}$, let

$$m(\mathbb{P}_i^{(k)}) = \begin{cases} y_i^{(k)} & 0 \leq k \leq \sum_{j=0}^{i-1} s_j \\ y_{i+1}^{(s_i+k)} & \sum_{j=0}^{i-1} s_j + 1 \leq k \leq s - s_i \end{cases}.$$

So $m(S_l)$ is equal to $\{y_j^{[s]} : 1 \leq j \leq n\}$, which are algebraically independent over \mathbb{Q} . Thus, the $n(s+1)$ members of S_l are algebraically independent over \mathbb{Q} . For if not, all the $\mathbb{P}_i^{(k)} - u_{i0}^{(k)}$ ($\mathbb{P}_i^{(k)} \in S_l$) are algebraically dependent over $\mathbb{Q}(\mathbf{v})$ where $\mathbf{v} = \cup_{i=0}^n \mathbf{u}_i^{[s-s_i]} \setminus \{u_{i0}^{[s-s_i]}\}$. Now specialize the coefficient of $m(\mathbb{P}_i^{(k)})$ in $\mathbb{P}_i^{(k)}$ to 1, and all the other coefficients of $\mathbb{P}_i^{(k)} - u_{i0}^{(k)}$ to 0, by the algebraic version of Lemma 2.2, $\{m(\mathbb{P}_i^{(k)}) : \mathbb{P}_i^{(k)} \in S_l\}$ are algebraically dependent over \mathbb{Q} , which is a contradiction. Thus, claim C1) is proved. Claim C2) follows from the fact that 1 and $\mathbb{Y}^{[s]}$ are contained in the support of $\mathbb{P}_0^{[s-s_0]}$.

By C1) and C2), the sparse resultant of $(\mathbb{P}_i^{(k)})_{0 \leq i \leq n; 0 \leq k \leq s-s_i}$ exists and we denote it by G . Then $(G) = ((\mathbb{P}_i^{(k)})_{0 \leq i \leq n; 0 \leq k \leq s-s_i}) \cap \mathbb{Q}[\mathbf{u}_0^{[s-s_0]}, \dots, \mathbf{u}_n^{[s-s_n]}]$, and by Theorem 6.4, $\deg(G, \mathbf{u}_i^{(k)}) = \mathcal{M}((\mathcal{Q}_{jl})_{j \neq i, 0 \leq l \leq s-s_j}, \mathcal{Q}_{i0}, \dots, \mathcal{Q}_{i, k-1}, \mathcal{Q}_{i, k+1}, \dots, \mathcal{Q}_{i, s-s_i})$, where $\mathbf{u}_i^{(k)} = (u_{i0}^{(k)}, \dots, u_{i\alpha}^{(k)}, \dots)$. The theorem will be proved if we can show that $G = c \cdot \mathbf{R}$ for some $c \in \mathbb{Q}$.

Since $G \in [\mathbb{P}_0, \dots, \mathbb{P}_n]$ and $\text{ord}(G, \mathbf{u}_i) = s - s_i$, by Lemma 3.9, $\text{ord}(\mathbf{R}, \mathbf{u}_i) \leq s - s_i$ for each $i = 0, \dots, n$. If for some i , $\text{ord}(\mathbf{R}, \mathbf{u}_i) = h_i < s - s_i$, then $\mathbf{R} \in ((\mathbb{P}_j^{(k)})_{j \neq i; 0 \leq k \leq s-s_j}, \mathbb{P}_i, \dots, \mathbb{P}_i^{(h_i)})$, a contradiction to C1). Thus, $\text{ord}(\mathbf{R}, \mathbf{u}_i) = s - s_i$ and $\mathbf{R} \in (G)$. Since \mathbf{R} is irreducible, there exists some $c \in \mathbb{Q}$ such that $G = c \cdot \mathbf{R}$. So \mathbf{R} is equal to the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \dots, \mathbb{P}_n^{[s-s_n]}$. \square

As a direct consequence of the above theorem and the determinant representation for algebraic sparse resultant given by D'Andrea [8], we have the following result.

Corollary 6.6 *The difference resultant for generic difference polynomials $\mathbb{P}_i, i = 0, \dots, n$ can be written as the form $\det(M_1)/\det(M_0)$ where M_1 and M_0 are matrixes whose elements are coefficients of \mathbb{P}_i and their transforms up to the order $s - s_i$ and M_0 is a minor of M_1 .*

Based on the matrix representation given in the above corollary, the single exponential algorithms given by Canny, Emiris, and Pan [11, 12] can be used to compute the difference resultant.

Remark 6.7 *From the proof of Theorem 6.5, we can see that for each i and $0 \leq k \leq s - s_i$, $\deg(\mathbf{R}, \mathbf{u}_i^{(k)}) > 0$. Furthermore, by Lemma 4.8, $\deg(\mathbf{R}, u_{i0}^{(k)}) > 0$ and $\deg(\mathbf{R}, u_{i\alpha}^{(k)}) > 0$ for each α . In particular, $\deg(\mathbf{R}, u_{i0}) > 0$ and $\deg(\mathbf{R}, u_{i\alpha}) > 0$.*

Now, we proceed to give a Poisson-type product formula for difference resultant. Let $\tilde{\mathbf{u}} = \cup_{i=0}^n \mathbf{u}_i \setminus \{u_{00}\}$ and $\mathbb{Q}(\tilde{\mathbf{u}})$ be the formally transcendental extension of \mathbb{Q} in the usual sense. Let $\mathbb{Q}_0 = \mathbb{Q}(\tilde{\mathbf{u}})(u_{00}, \dots, u_{00}^{(s-s_0-1)})$. Here, \mathbb{Q}_0 is not necessarily a difference overfield of \mathbb{Q} , for the transforms of u_{00} are not defined. In the following, we will follow Cohn [4] to obtain algebraic extensions \mathcal{G}_i of \mathbb{Q}_0 and define transforming operators to make \mathcal{G}_i difference fields. Consider \mathbf{R} as an irreducible algebraic polynomial $r(u_{00}^{(s-s_0)})$ in $\mathbb{Q}_0[u_{00}^{(s-s_0)}]$. In a suitable

algebraic extension field of \mathbb{Q}_0 , $r(u_{00}^{(s-s_0)}) = 0$ has $t_0 = \deg(r, u_{00}^{(s-s_0)}) = \deg(\mathbf{R}, u_{00}^{(s-s_0)})$ roots $\gamma_1, \dots, \gamma_{t_0}$. Thus

$$\mathbf{R}(\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_n) = A \prod_{\tau=1}^{t_0} (u_{00}^{(s-s_0)} - \gamma_\tau) \quad (16)$$

where $A \in \mathbb{Q}_0$. Let $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$. Then by Definition 6.2, $\mathcal{I}_{\mathbf{u}}$ is an essential reflexive prime difference ideal in the decomposition of $\{\mathbf{R}\}$ which is not held by any difference polynomial of order less than $s - s_0$ in u_{00} . Suppose $\mathbf{R}, \mathbf{R}_1, \mathbf{R}_2, \dots$ is a basic sequence¹ of \mathbf{R} corresponding to $\mathcal{I}_{\mathbf{u}}$. That is, $\mathcal{I}_{\mathbf{u}} = \bigcup_{k \geq 0} \text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$. Regard all the \mathbf{R}_i as algebraic polynomials over the coefficient field $\mathbb{Q}\langle \tilde{\mathbf{u}} \rangle$. Denote $\gamma_{\tau 0} = \gamma_\tau$. Clearly, $u_{00}^{(s-s_0)} = \gamma_{\tau 0}$ is a generic point of $\text{asat}(\mathbf{R})$. Suppose $\gamma_{\tau i}$ ($i \leq k$) are found in some algebraic extension field of \mathbb{Q}_0 such that $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ ($0 \leq i \leq k$) is a generic point of $\text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$. Then let $\gamma_{\tau, k+1}$ be an element such that $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ ($0 \leq i \leq k+1$) is a generic point of $\text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k, \mathbf{R}_{k+1})$. Clearly, $\gamma_{\tau, k+1}$ is also algebraic over \mathbb{Q}_0 . Let $\mathcal{G}_\tau = \mathbb{Q}\langle \tilde{\mathbf{u}} \rangle(u_{00}, \dots, u_{00}^{(s-s_0-1)}, \gamma_\tau, \gamma_{\tau 1}, \dots)$. Clearly, \mathcal{G}_τ is an algebraic extension of \mathbb{Q}_0 and \mathcal{G}_τ is algebraically isomorphic to the quotient field of $\mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}/\mathcal{I}_{\mathbf{u}}$. Since the quotient field of $\mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}/\mathcal{I}_{\mathbf{u}}$ is also a difference field, we can introduce a transforming operator σ_τ into \mathcal{G}_τ to make it a difference field such that the above isomorphism becomes a difference one. That is, $\sigma_\tau|_{\mathbb{Q}_0} = \text{id}_{\mathbb{Q}_0}$ and

$$\sigma_\tau^k(u_{00}) = \begin{cases} u_{00}^{(k)} & 0 \leq k \leq s - s_0 - 1 \\ \gamma_{\tau, k-s-s_0} & k \geq s - s_0 \end{cases}$$

In this way, $(\mathcal{G}_\tau, \sigma_\tau)$ is a difference field.

Let F be a difference polynomial in $\mathbb{Q}\{\mathbf{u}_0, \mathbf{u}_1, \dots, \mathbf{u}_n\} = \mathbb{Q}\{\tilde{\mathbf{u}}, u_{00}\}$. For convenience, by the symbol $F|_{u_{00}^{(s-s_0)}=\gamma_\tau}$, we mean substituting $u_{00}^{(s-s_0+k)}$ by $\sigma_\tau^k \gamma_\tau = \gamma_{\tau k}$ ($k \geq 0$) into F . Similarly, by saying F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$, we mean $F|_{u_{00}^{(s-s_0)}=\gamma_\tau} = 0$. The following lemma is a direct consequence of the above discussion.

Lemma 6.8 *$F \in \mathcal{I}_{\mathbf{u}}$ if and only if F vanishes at $u_{00}^{(s-s_0)} = \gamma_\tau$.*

Proof: Since $\mathcal{I}_{\mathbf{u}} = \bigcup_{k \geq 0} \text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$ and $u_{00}^{(s-s_0+i)} = \gamma_{\tau i}$ ($0 \leq i \leq k$) is a generic point of $\text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$, the lemma follows. \square

Remark 6.9 *In order to make \mathcal{G}_τ a difference field, we need to introduce a transforming operator σ_τ which is closely related to γ_τ . Since even for a fixed τ , generic points of $\text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$ beginning from $u_{00}^{(s-s_0)} = \gamma_\tau$ may not be unique, the definition of σ_τ also may not be unique, which is different from the differential case. In fact, it is a common phenomena in difference algebra. Here, we just choose one, for they do not influence the following discussions.*

¹For the rigorous definition of *basic sequence*, please refer to [4]. Here, we list its basic properties: i) For each $k \geq 0$, $\text{ord}(\mathbf{R}_k, u_{00}) = s - s_0 + k$ and $\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k$ is an irreducible algebraic ascending chain, and ii) $\bigcup_{k \geq 0} \text{asat}(\mathbf{R}, \mathbf{R}_1, \dots, \mathbf{R}_k)$ is a reflexive prime difference ideal.

Now we give the following Poisson type formula for the difference resultant.

Theorem 6.10 *Let $\mathbf{R}(\mathbf{u}_0, \dots, \mathbf{u}_n)$ be the difference resultant of $\mathbb{P}_0, \dots, \mathbb{P}_n$. Let $\deg(\mathbf{R}, u_{00}^{(s-s_0)}) = t_0$. Then there exist $\xi_{\tau k}$ ($\tau = 1, \dots, t_0; k = 1, \dots, n$) in overfields $(\mathcal{G}_\tau, \sigma_\tau)$ of $(\mathbb{Q}\langle \hat{\mathbf{u}} \rangle, \sigma)$ such that*

$$\mathbf{R} = A \prod_{\tau=1}^{t_0} \mathbb{P}_0(\xi_{\tau 1}, \dots, \xi_{\tau n})^{(s-s_0)}, \quad (17)$$

where $A \in \mathbb{Q}\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle[u_{00}^{[s-s_0]} \setminus u_{00}^{(s-s_0)}]$. Note that (17) is formal and should be understood in the following precise meaning: $\mathbb{P}_0(\xi_{\tau 1}, \dots, \xi_{\tau n})^{(s-s_0)} \triangleq \sigma^{s-s_0} u_{00} + \sigma_\tau^{s-s_0} (\sum_\alpha u_{0\alpha} (\xi_\tau^{[s-s_0]})^\alpha)$, where $\xi_\tau = (\xi_{\tau 1}, \dots, \xi_{\tau n})$.

Proof: By Theorem 4.7, there exists $m \in \mathbb{N}$ such that

$$u_{00} \frac{\partial \mathbf{R}}{\partial u_{00}} + \sum_\alpha u_{0\alpha} \frac{\partial \mathbf{R}}{\partial u_{0\alpha}} = m \mathbf{R}.$$

Setting $u_{00}^{(s-s_0)} = \gamma_\tau$ in both sides of the above equation, we have

$$u_{00} \frac{\partial \mathbf{R}}{\partial u_{00}} \Big|_{u_{00}^{(s-s_0)} = \gamma_\tau} + \sum_\alpha u_{0\alpha} \frac{\partial \mathbf{R}}{\partial u_{0\alpha}} \Big|_{u_{00}^{(s-s_0)} = \gamma_\tau} = 0.$$

Let $\xi_{\tau\alpha} = (\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} / \frac{\partial \mathbf{R}}{\partial u_{00}}) \Big|_{u_{00}^{(s-s_0)} = \gamma_\tau}$. Then $u_{00} = -\sum_\alpha u_{0\alpha} \xi_{\tau\alpha}$ with $u_{00}^{(s-s_0)} = \gamma_\tau$. That is, $\gamma_\tau = -\sigma_\tau^{s-s_0} (\sum_\alpha u_{0\alpha} \xi_{\tau\alpha}) = -(\sum_\alpha u_{0\alpha} \xi_{\tau\alpha})^{(s-s_0)}$. Thus,

$$\mathbf{R} = A \prod_{\tau=1}^{t_0} (u_{00} + \sum_\alpha u_{0\alpha} \xi_{\tau\alpha})^{(s-s_0)}.$$

Suppose $\mathbb{P}_0 = u_{00} + \sum_{j=1}^n u_{0j} y_j + T_0$. Let $\xi_{\tau j} = (\frac{\partial \mathbf{R}}{\partial u_{0j}} / \frac{\partial \mathbf{R}}{\partial u_{00}}) \Big|_{u_{00}^{(s-s_0)} = \gamma_\tau}$ ($j = 1, \dots, n$) and $\xi_\tau = (\xi_{\tau 1}, \dots, \xi_{\tau n})$. It remains to show that $\xi_{\tau\alpha} = (\xi_\tau^{[s_0]})^\alpha$.

Let $\zeta_i = -\sum_\alpha u_{i\alpha} (\mathbb{Y}^{[s_i]})^\alpha$ ($i = 0, \dots, n$). Clearly, $\zeta = (\mathbf{u}, \zeta_0, \dots, \zeta_n)$ is a generic point of $\mathcal{I}_{\mathbf{u}} = [\mathbb{P}_0, \dots, \mathbb{P}_n] \cap \mathbb{Q}\{\mathbf{u}_0, \dots, \mathbf{u}_n\}$, where $\mathbf{u} = \cup_{i=1}^n \mathbf{u}_i \setminus \{u_{i0}\}$. For each $(\mathbb{Y}^{[s_0]})^\alpha = \prod_{j=1}^n (y_j^{(k)})^{d_{jk}}$, by equation (7), $(\mathbb{Y}^{[s_0]})^\alpha = \frac{\overline{\partial \mathbf{R}}}{\partial u_{0\alpha}} / \frac{\overline{\partial \mathbf{R}}}{\partial u_{00}} = \prod_{j=1}^n \prod_{k=0}^{s_0} \left(\left(\frac{\overline{\partial \mathbf{R}}}{\partial u_{0j0}} / \frac{\overline{\partial \mathbf{R}}}{\partial u_{00}} \right)^{(k)} \right)^{d_{jk}}$, where $\frac{\overline{\partial \mathbf{R}}}{\partial u_{0\alpha}} = \frac{\partial \mathbf{R}}{\partial u_{0\alpha}} \Big|_{u_{i0} = \zeta_i}$. So $\frac{\partial \mathbf{R}}{\partial u_{0\alpha}} \prod_{j=1}^n \prod_{k=0}^{s_0} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{0j0}} \right)^{(k)} \right)^{d_{jk}} - \frac{\partial \mathbf{R}}{\partial u_{00}} \prod_{j=1}^n \prod_{k=0}^{s_0} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{0j0}} \right)^{(k)} \right)^{d_{jk}} \in \mathcal{I}_{\mathbf{u}}$. By Lemma 6.8, $\xi_{\tau\alpha} = \prod_{j=1}^n \prod_{k=0}^{s_0} (\xi_{\tau j}^{(k)})^{d_{jk}} = (\xi_\tau^{[s_0]})^\alpha$. Thus, (17) follows. \square

Theorem 6.11 *The points $\xi_\tau = (\xi_{\tau 1}, \dots, \xi_{\tau n})$ ($\tau = 1, \dots, t_0$) in (17) are generic points of the difference ideal $[\mathbb{P}_1, \dots, \mathbb{P}_n] \subset \mathbb{Q}\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle \{ \mathbb{Y} \}$.*

Proof: Clearly, ξ_τ are n -tuples over $\mathbb{Q}\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle$. For each $i = 1, \dots, n$, rewrite $\mathbb{P}_i = u_{i0} + \sum_{\alpha} u_{i\alpha} \prod_{j=1}^n \prod_{k=1}^{s_i} (y_j^{(k)})^{\alpha_{jk}}$. Since $\zeta_i = -\sum_{\alpha} u_{i\alpha} \prod_{j=1}^n \prod_{k=1}^{s_i} (y_j^{(k)})^{\alpha_{jk}}$ and $y_j = \frac{\partial \mathbf{R}}{\partial u_{0j0}} / \frac{\partial \mathbf{R}}{\partial u_{00}}$, $\zeta_i + \sum_{\alpha} u_{i\alpha} \prod_{j=1}^n \prod_{k=1}^{s_i} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{0j0}} / \frac{\partial \mathbf{R}}{\partial u_{00}} \right)^{(k)} \right)^{\alpha_{jk}} = 0$. Let $a_{jk} = \max_{\alpha} \alpha_{jk}$. Then $u_{i0} \prod_{j=1}^n \prod_{k=1}^{s_i} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{00}} \right)^{(k)} \right)^{a_{jk}} + \sum_{\alpha} u_{i\alpha} \prod_{j=1}^n \prod_{k=1}^{s_i} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{0j0}} \right)^{(k)} \right)^{\alpha_{jk}} \left(\left(\frac{\partial \mathbf{R}}{\partial u_{00}} \right)^{(k)} \right)^{a_{jk} - \alpha_{jk}} \in \mathcal{I}_{\mathbf{u}}$. Thus, by Lemma 6.8, $\mathbb{P}_i(\xi_\tau) = u_{i0} + \sum_{\alpha} u_{i\alpha} \prod_{j=1}^n \prod_{k=1}^{s_i} (\xi_{\tau j}^{(k)})^{\alpha_{jk}} = 0$ ($i = 1, \dots, n$).

On the other hand, suppose $F \in \mathbb{Q}\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle \{\mathbb{Y}\}$ vanishes at ξ_τ . Without loss of generality, suppose $F \in \mathbb{Q}\{\mathbf{u}_1, \dots, \mathbf{u}_n, \mathbb{Y}\}$. Clearly, $\mathbb{P}_1, \dots, \mathbb{P}_n$ constitute an ascending chain in $\mathbb{Q}\{\mathbf{u}_1, \dots, \mathbf{u}_n, \mathbb{Y}\}$ with u_{i0} as leaders. Let G be the difference remainder of F with respect to this ascending chain. Then G is free from u_{i0} and $F \equiv G \pmod{[\mathbb{P}_1, \dots, \mathbb{P}_n]}$. Then $G(\xi_\tau) = G(\tilde{\mathbf{u}}; \xi_{\tau 1}, \dots, \xi_{\tau n}) = 0$, where $\tilde{\mathbf{u}} = \cup_{i=1}^n \mathbf{u}_i \setminus \{u_{i0}\}$. So there exist $a_k \in \mathbb{N}$ such that $G_1 = \prod_k \left(\left(\frac{\partial \mathbf{R}}{\partial u_{00}} \right)^{(k)} \right)^{a_k} G(\tilde{\mathbf{u}}; \mathbb{Y}) \in \mathcal{I}_{\mathbf{u}}$. Thus, G_1 vanishes at $u_{i0} = \zeta_i$ ($i = 1, \dots, n$) while $\frac{\partial \mathbf{R}}{\partial u_{00}}$ does not. It follows that $G(\tilde{\mathbf{u}}; \mathbb{Y}) \equiv 0$ and $F \in [\mathbb{P}_1, \dots, \mathbb{P}_n]$. So ξ_τ are generic points of $[\mathbb{P}_1, \dots, \mathbb{P}_n] \subset \mathbb{Q}\langle \mathbf{u}_1, \dots, \mathbf{u}_n \rangle \{\mathbb{Y}\}$. \square

By Theorem 6.10 and 6.11, we can see that difference resultants have Poisson-type product formula which is similar to their algebraic and differential analogues.

7 Conclusion and problem

In this paper, we first introduce the concepts of Laurent difference polynomials and Laurent transformally essential systems and give a criterion for Laurent transformally essential systems in terms of their supports. Then the sparse difference resultant for a Laurent transformally essential system is defined and its basic properties are proved. Furthermore, order and degree bounds for the sparse difference resultant are given. Based on these bounds, an algorithm to compute the sparse difference resultant is proposed, which is single exponential in terms of the order, the number of variables, and the size of the Laurent transformally essential system. Besides these, the difference resultant is introduced and its basic properties are given, such as its precise order, degree, determinant representation and the Poisson-type product formula.

In the rest of this section, we propose several questions for further study apart from Problem 3.15.

It is useful to represent the sparse difference resultant as the quotient of two determinants, as done in [8, 11] in the algebraic case. In the difference case, Theorem 6.5 shows that difference resultant has such a matrix formula, but for sparse difference resultant, we do not have such a formula yet. From (11), a natural idea to find a matrix representation is trying to define the sparse difference resultant as the algebraic sparse resultant of $\mathbb{P} = \{\mathbb{P}_i^{(k)} (i = 0, \dots, n, k = 0, \dots, h_i)\}$ considered as Laurent polynomials in $y_l^{(j)}$.

The degree of the algebraic sparse resultant is equal to the mixed volume of certain polytopes generated by the supports of the polynomials [24] or [16, p.255]. A similar degree bound is given [23, Theorem 1.3] for the differential resultant. And Theorem 6.5 shows that

the degree of difference resultants is exactly of such BKK-type. We conjecture that sparse difference resultant has such degree bounds.

There exist very efficient algorithms to compute algebraic sparse resultants [10, 11, 12, 8], which are based on matrix representations for the resultant. How to apply the principles behind these algorithms to compute sparse difference resultants is an important problem.

References

- [1] D. N. Bernshtein. The Number of Roots of a System of Equations. *Functional Anal. Appl.*, 9(3), 183-185, 1975.
- [2] D. Bouziane, A. Kandri Rody, and H. Maârouf. Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. *Journal of Symbolic Computation*, 31(6), 631-649, 2001.
- [3] J. F. Canny. Generalized Characteristic Polynomials. *Journal of Symbolic Computation*, 9, 241-250, 1990.
- [4] R. M. Cohn. Manifolds of Difference Polynomials. *Trans. Amer. Math. Soc.*, 64(1), 1948.
- [5] R. M. Cohn. *Difference Algebra*. Interscience Publishers, New York, 1965.
- [6] R. M. Cohn. Order and Dimension. *Proc. Amer. Math. Soc.*, 87(1), 1983.
- [7] D. Cox, J. Little, D. O'Shea. *Using Algebraic Geometry*. Springer, 1998.
- [8] C. D'Andrea. Macaulay Style Formulas for Sparse Resultants. *Trans. of AMS*, 354(7), 2595-2629, 2002.
- [9] D. Eisenbud, F. O. Schreyer, and J. Weyman. Resultants and Chow Forms via Exterior Syzygies. *Journal of Amer. Math. Soc.*, 16(3), 537-579, 2004.
- [10] I. Z. Emiris. On the Complexity of Sparse Elimination. *J. Complexity*, 12, 134-166, 1996.
- [11] I. Z. Emiris and J. F. Canny. Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume. *Journal of Symbolic Computation*, 20(2), 117-149, 1995.
- [12] I. Z. Emiris and V. Y. Pan. Improved algorithms for computing determinants and resultants. *Journal of Complexity*, 21, 43-71, 2005.
- [13] X. S. Gao and S. C. Chou. On the Dimension for Arbitrary Ascending Chains. *Chinese Bull. of Sciences*, vol. 38, 396-399, 1993.
- [14] X. S. Gao, W. Li, C. M. Yuan. Intersection Theory in Differential Algebraic Geometry: Generic Intersections and the Differential Chow Form. *arXiv:1009.0148v2*, 58 pages, 2011, accepted by *Trans. of Amer. Math. Soc.*.
- [15] X. S. Gao, Y. Luo, C. M. Yuan. A Characteristicset Method for Ordinary Difference Polynomial Systems. *Journal of Symbolic Computation*, 44(3), 242-260, 2009.

- [16] I. M. Gelfand, M. Kapranov, A. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants*. Boston, Birkhäuser, 1994.
- [17] W.V.D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume I*. Cambridge Univ. Press, 1968.
- [18] J. P. Jouanolou. Le formalisme du résultant. *Advances in Mathematics*, 90(2), 117-263, 1991.
- [19] M. Kapranov, B. Sturmfels, and A. Zelevinsky. Chow Polytopes and General Resultants. *Duke Math. J.*, 67, 189-218, 1992.
- [20] B. A. Lando. Jacobi's Bound for the Order of Systems of First Order Differential Equations. *Trans. Amer. Math. Soc.* 152, 119-135, 1970.
- [21] A. Levin. *Difference Algebra*. Springer, 2008.
- [22] W. Li, X. S. Gao, C. M. Yuan. Sparse Differential Resultant. *Proc. ISSAC 2011*, 225-232, ACM Press, New York, 2011.
- [23] W. Li, C. M. Yuan, X. S. Gao. Sparse Differential Resultant for Laurent Differential Polynomials. *arXiv:1111.1084v3*, 70 pages, 2012.
- [24] P. Pedersen and B. Sturmfels. Product Formulas for Resultants and Chow Forms. *Mathematische Zeitschrift*, 214(1), 377-396, 1993.
- [25] S. L. Rueda. Linear Sparse Differential Resultant Formulas. *arXiv:1112.3921v2*, 2011.
- [26] B. Sturmfels. Sparse Elimination Theory. In *Computational Algebraic Geometry and Commutative Algebra*, Eisenbud, D., Robbiano, L. eds. 264-298, Cambridge University Press, 1993.
- [27] B. Sturmfels. On The Newton Polytope of the Resultant. *Journal of Algebraic Combinatorics*, 3, 207-236, 1994.
- [28] W. Vogel. *Lectures on Results on Bezout's Theorem*. Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1984.
- [29] W. T. Wu. *Mathematics Machenization*. Science Press/Kluwer, Beijing, 2003.
- [30] Z. Y. Zhang, C. M. Yuan, X. S. Gao. Matrix Formula of Differential Resultant for First Order Generic Ordinary Differential Polynomials. *arXiv:1204.3773*, 2012.